IJCSIS Vol. 10 No. 7, July 2012
ISSN 1947-5500

International Journal of Computer Science & Information Security

© IJCSIS PUBLICATION 2012


Cornell University
Library


Cogprints


Google scholar


.docstoc
find and share professional documents


ScientificCommons

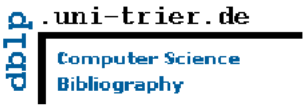

View my documents on
Scribd


BASE
Bielefeld Academic Search Engine


SCIRUS
search engine for science


SciRate.com


CiteSeerx beta


dblp .uni-trier.de
Computer Science
Bibliography


Q·Sensei


DOAJ
DIRECTORY OF
OPEN ACCESS
JOURNALS


EBSCO
HOST


ProQuest

Editorial
Message from Managing Editor

*The **International Journal of Computer Science and Information Security** (IJCSIS) is a well-established and notable venue for publishing high quality research papers as recognised by various universities and international professional bodies. IJCSIS is a refereed open access international journal for publishing scientific papers in all areas of computer science research. IJCSIS publishes original research works and reviewed articles in all areas of computer science including emerging topics like cloud computing, software development etc. The journal promotes insight and understanding of the state of the art and trends in computing technology and applications.*

IJCSIS solicits authors/researchers/scholars to contribute to the journal by submitting articles that illustrate research results, projects, surveying works and industrial experiences. IJCSIS helps academia promptly publish academic work to sustain or further one's career.

For complete details about IJCSIS archives publications, abstracting/indexing, editorial board and other important information, please refer to IJCSIS homepage. IJCSIS appreciates all the insights and advice from authors/readers and reviewers. Indexed by the following International Agencies and institutions: Google Scholar, Bielefeld Academic Search Engine (BASE), CiteSeerX, SCIRUS, Cornell's University Library EI, Scopus, DBLP, DOI, ProQuest.

Google Scholar reported a large amount of cited papers published in IJCSIS. We will continue to encourage the readers, authors and reviewers and the computer science scientific community and authors to continue citing papers published by the journal. Considering the growing interest of academics worldwide to publish in IJCSIS, we invite universities and institutions to partner with us to further encourage open-access publications

*We look forward to receive your valuable papers. The topics covered by this journal are diverse. (See monthly Call for Papers). If you have further questions please do not hesitate to contact us at **ijcsiseditor@gmail.com**. Our team is committed to provide a quick and supportive service throughout the publication process.*

A complete list of journals can be found at:
http://sites.google.com/site/ijcsis/

IJCSIS Vol. 10, No. 7, July 2012 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):



IJCSIS EDITORIAL BOARD

Dr. Yong Li
School of Electronic and Information Engineering, Beijing Jiaotong University, P. R. China

Prof. Hamid Reza Naji
Department of Computer Enigneering, Shahid Beheshti University, Tehran, Iran

Dr. Sanjay Jasola
Professor and Dean, School of Information and Communication Technology, Gautam Buddha University

Dr Riktesh Srivastava
Assistant Professor, Information Systems, Skyline University College, University City of Sharjah, Sharjah, PO 1797, UAE

Dr. Siddhivinayak Kulkarni
University of Ballarat, Ballarat, Victoria, Australia

Professor (Dr) Mokhtar Beldjehem
Sainte-Anne University, Halifax, NS, Canada

Dr. Alex Pappachen James (Research Fellow)
Queensland Micro-nanotechnology center, Griffith University, Australia

Dr. T. C. Manjunath
HKBK College of Engg., Bangalore, India.

Prof. Elboukhari Mohamed
Department of Computer Science,
University Mohammed First, Oujda, Morocco



TABLE OF CONTENTS

1. Paper 24061207: A Low Cost PC-Controlled Electronic-Display Board (pp. 1-4)

M. G. Golam Faruque, Bangladesh Computer Council, Dhaka, Bangladesh
Shamim Ahmad, Dept. of Computer Scienec and Engineering, Rajshahi University, Rajshahi, Bangladesh

Abstract — This paper describes the development of a computer controlled electronic display-board by using a low cost older personal computer (PC) that has become almost unusable otherwise. This display system is capable to display the information as an independent system in the manner that can be dynamically programmed by the computer. A local control system, memory-subsystem has been developed to make it to work as an independent system.

2. Paper 30061215: An Approach be Operational Security in 3 and 4 Phases of Developing Software Systems (pp. 5-11)

Saman Aleshi, Dept. Department of Electrical and Computer, Islamic Azad University, Zanjan Branch, Zanjan, Iran
Nasser Modiri, Dept. Department of Electrical and Computer, Islamic Azad University, Zanjan Branch, Zanjan, Iran
Hossein Fruzi, Dept. Department of Electrical and Computer, Islamic Azad University, Zanjan Branch, Zanjan, Iran

Abstract - Security in today's software applications because raw data acquisition system at the lowest level, the position is very important however, part of the development application under consideration is the security and therefore also delirium costs have to using and user. Security is essential in software development because the resource is protected to the integrity, availability and privacy of data guarantee. There are different models and standards for information security. PSSS is one of those models specialized for providing security tasks in PSSS, as an efficient software security model, in order to map in along with other security models and standard for 3 and 4 phases of software development, ensuring safety of task performance in the phases.

Keywords - IT (Information Technology), IT security, Security Models and Standards and their limitations.

3. Paper 30061225: Analysis & Selection of Requirements Elicitation Techniques for OSSD (pp. 12-22)

Munazza Ishtiaq, Fareeha Choudhry, Fahim Ashraf Awan, Aasia Khanum
Department of Computer Engineering, College of Electrical & Mechanical Engineering, National University of Sciences and Technology (NUST), Rawalpindi, Pakistan

Abstract — Open Source Software development (OSSD) is unlike traditional software development in many aspects. Requirements elicitation is the most critical phase in software development as it is the basis for developing software. The requirements elicitation phase in OSSD is different from traditional software development process and somehow a difficult process as the developer is the only person that has to elicit the requirements and then make the software open for review from the user community. The users can add or modify the product according to their own needs and requirements. The focus of this paper is on the requirements elicitation phase and elicitation techniques for open source software development. In this paper, requirements elicitation phase model for OSSD is proposed as well as best suited requirements elicitation techniques for OSSD are discussed and a framework for choosing and comparing these techniques is developed and the selected techniques for OSS are analyzed in the context of the criteria mentioned in the framework. A formula is proposed using the framework and the proposed model for the requirements elicitation process and selection of techniques for OSSD.

Keywords — framework, OSSD, requirements elicitation process model, requirements elicitation techniques, traditional software development

4. Paper 30061229: Log Analysis Techniques using Clustering in Network Forensics (pp. 23-30)

Imam Riadi, Faculty of Mathematics and Natural Science, Ahmad Dahlan University, Yogyakarta, Indonesia
Jazi Eko Istiyanto & Ahmad Ashari, Subanar, Faculty of Mathematics and Natural Sciences, Gadjah Mada University, Yogyakarta, Indonesia

Abstract — Internet crimes are now increasing. In a row with many crimes using information technology, in particular those using Internet, some crimes are often carried out in the form of attacks that occur within a particular agency or institution. To be able to find and identify the types of attacks, requires a long process that requires time, human resources and utilization of information technology to solve these problems. The process of identifying attacks that happened also needs the support of both hardware and software as well. The attack happened in the Internet network can generally be stored in a log file that has a specific data format. Clustering technique is one of methods that can be used to facilitate the identification process. Having grouped the data log file using K-means clustering technique, then the data is grouped into three categories of attack, and will be continued with the forensic process that can later be known to the source and target of attacks that exist in the network. It is concluded that the framework proposed can help the investigator in the trial process.

Keywords: analysis, network, forensic, clustering, attack

5. Paper 30061230: A Comparative Study between Using OWL Technology and Jess Rule Based For Applying Knowledge to Agent Based System (pp. 31-37)

Najla Badie Aldabagh & Ban Sharief Mustafa, Computer Sciences Department, Mosul University Iraq, Mosul

Abstract — The Semantic Web is an extended to the current web where web resources can be manipulated and processed intelligently. User query is semantically analyzed and respond to in intelligent way. A set of technologies are developed to serve this requirement, including Resource Description Framework (RDF), Schema RDF and Web Ontology Language (OWL). Java Agent Development Framework (JADE) is a software framework to make easy the development of multi agent applications in compliance with The Foundation for Intelligent Physical Agents (FIPA) specifications. Several approaches for building knowledge model for JADE agent can be found. The most promising approach is using OWL ontology based knowledge representation which is one of the main standards for the Semantic Web proposed by World Wide Web Consortium (W3C), and it is based on description logic. Representing knowledge based on ontology provides many benefits over other representations. The other traditional approach is using conventional rule engine (normally production rule engine). Jess is a familiar rule engine and scripting environment written entirely in Sun's java language. Jess gives the capability for building Knowledge in the form of declarative rules and facts, and reason about it. Also Jess can be integrated efficiently with a JADE agent. In this paper, A comparative study is held between the above two approaches. An example is implemented to show the tools and steps required in each way and to show the expressivity power of the ontology based over the traditional one.

Keywords-component; Java Agent Development Framework (JADE); Web Ontology Language (OWL); Jess; Knowledge Representation; Description Logic (DL).

6. Paper 30061233: Modeling and Control of CSTR using Model based Neural Network Predictive Control (pp. 38-43)

Piyush Shrivastava, Electrical& Electronics Engineering Department, Takshshila Institute of Engineering & Technology, Jabalpur, Madhya Pradesh, India

Abstract — This paper presents a predictive control strategy based on neural network model of the plant is applied to Continuous Stirred Tank Reactor (CSTR). This system is a highly nonlinear process; therefore, a nonlinear predictive method, e.g., neural network predictive control, can be a better match to govern the system dynamics. In

the paper, the NN model and the way in which it can be used to predict the behavior of the CSTR process over a certain prediction horizon are described, and some comments about the optimization procedure are made. Predictive control algorithm is applied to control the concentration in a continuous stirred tank reactor (CSTR), whose parameters are optimally determined by solving quadratic performance index using the optimization algorithm. An efficient control of the product concentration in CSTR can be achieved only through accurate model. Here an attempt is made to alleviate the modeling difficulties using Artificial Intelligent technique such as Neural Network. Simulation results demonstrate the feasibility and effectiveness of the NNMPC technique.

Keywords - Continuous Stirred Tank Reactor; Neural Network based Predictive Control; Nonlinear Auto Regressive with eXogenous signal.

7. Paper 30061235: Visualization for levels of animal diseases by integrating OLAP and GIS (pp. 44-50)

Prof. Hesham Ahmed Hassan, Faculty of Computer and Information, Cairo University, Giza, Egypt
Dr. Hazem El-Bakry, Faculty of Computer and Information, Mansoura University, Mansoura, Egypt
Mr. Hamada Gaber Abd Allah, Faculty of Computer and Information, Cairo, Egypt

Abstract - Animal diseases have constituted a major problem in many developing and developed countries. There are different limitations for the existing computer systems to meet the required information and analytical capabilities for a better decision in the Egyptian animal production domain. This paper presents an approach for helping policy/decision makers to improve animal production in Egypt. The paper integrates Online Analytical Processing (OLAP), Geographical Information System (GIS), Spatial Analysis functions and Multicriteria Decision Analysis (MCDA) capabilities to develop a Spatial Decision Support System (SDSS). The main aim of this study is to generate a composite map for decision makers by using some effective factors affect animal production in Egypt. We visualize and analyze different factors such as "*Diseases*", "*Climate*", "*Soil Pollution*", "*Veterinary care*" and "*Economical factors*" which affect the animal production in Egypt. The paper takes in consideration influence of each factor because importance and influence of each factor differs according policy/decision makers point of view.

Keywords: Geographical Information System (GIS),Multicriteria Decision Analysis (MCDA), Online Analytical Processing (OLAP), Spatial Analysis and Spatial Decision Support System (SDSS).

8. Paper 30061237: The Agents scrutiny at Protocol Stack in NIDS (pp. 51-57)

Mr. M. Shiva Kumar, Dept. of CSE/Karpagam University/Coimbatore/T.N,
Dr. K. Krishnamoorthy, Dept. of CSE/ Kuppam Engineering College/Kuppam/A.P

Abstract - The Research on the betterment of IDS and IPS is an avalanche process wherein each footstep paves way for new research work. In this regard This paper is a survey sheet on my research with respect to the implementation of Agents in the NIDS, first the paper depicts the OSI, later the impact of NIDS and the implementation of Agents in NIDS and it give a overview of the role of Agents in Basic Security Model and OSI reference and TCP/IP Model

Keywords : IDS,IPS,NIDS,TCP,IP,OSI.

9. Paper 30061241: Analytical study to Measure Employee satisfaction in Jordan e-government applications *E- Diwan Project- in prime minister office in Jordan* (pp. 58-62)

Bashar H. Sarayreh, Management Information Systems Department, Information Technology College, Arab Academy for Banking and Financial Sciences, Amman Jordan
Mohamad M. Al-Laham, Al-Balqa Applied University, Amman University College, MIS Department , Amman, Jordan

Abstract— There is a tremendous need by governments around the world to take advantage of the information revolution particularly the field of Enterprise resource planning and E-government in ordered to attain the optimum

method of recourses investment. Traditionally e-government development is organized in to different phases (requirements, analysis, design, implementation, testing and maintenance). To assess whether e-government models we implementing meets all different user requirements in order to increase user performance. E-government model with a large diversity of users suffer from failures to satisfy heterogeneous requirements. A solution for this damaging situation is by deeply and in detail studying and analyzing user satisfaction factors. The future development try to avoid such unsatisfied factors which disturb user and minimized there performance. E-government is considered as hot topic tackled by many researchers as it is considered as future fact especially for the developing countries. This research introduces a case study: Analytical study to Measure Employee satisfaction in Jordan e-government applications: E- Diwan Project- in prime minister office in Jordan.

Keywords: e-government, Satisfaction, E-Diwani, ERP

10. Paper 30051215: Bio-thentic Card: Authentication Concept For RFID Card (pp. 63-68)

Ikuesan Richard Adeyemi, Dept. computer science and information system, Universiti Teknologi, Malaysia, Johor Bahru, Malaysia
Norafida Bt, Ithnin, Dept. computer science and information system, Universiti Teknologi, Malaysia, Johor Bahru, Malaysia

Abstract - Radio frequency identification (RFID) is a technology that employs basic identifier of an object embedded in a chip, transmitted via radio wave, for identification. An RFID Card responds to query/interrogation irrespective of 'Who' holds the Card; like a key to a door. Since an attacker can possess the card, access to such object can therefore be easily compromised. This security breach is classified as an unauthorized use of Card, and it forms the bedrock for RFID Card compromise especially in access control. As an on-card authentication mechanism, this research proposed a concept termed Bio-thentic Card, which can be adopted to prevent this single point of failure of RFID Card. The Bio-thentic Card was fabricated, tested and assessed in line with the known threats, and attacks; and it was observed to proffer substantive solution to unauthorized use of RFID Card vulnerability.

Keywords: Vulnerability, unauthorized, mitigation, authentication, communication, access control system

11. Paper 26061209: ARP Cache Poisoning Attack and Detection (pp. 69-79)

Fatimah mohammed Al-Qarni, Computer Science and Engineering, Yanbu University College

A Low Cost PC-Controlled Electronic-Display Board

M. G. Golam Faruque
Bangladesh Computer Council
Dhaka, Bangladesh
golam_faruq @yahoo.com

Shamim Ahmad
Dept. of Computer Scienec and Engineering
Rajshahi University
Rajshahi, Bangladesh
shamim_cst)@yahoo.com

***Abstract*— This paper describes the development of a computer controlled electronic display-board by using a low cost older personal computer (PC) that has become almost unusable otherwise. This display system is capable to display the information as an independent system in the manner that can be dynamically programmed by the computer. A local control system, memory-subsystem has been developed to make it to work as an independent system.**

I. INTRODUCTION

An electronic-display board is a two-dimensional LED-array system in which each LED [1] acts as a pixel, therefore, any text or image can be displayed on that board. In the modern days, this type electronic-display boards are being used widely for different type of applications, for example, just for displaying fixed contents for advertising or information delivery. These first types of electronic-display board are static in the sense that once these boards are programmed to display some contents; it will continue to display those contents until it is reprogrammed. On the other hand, some electronic display-board are said to be dynamic in the sense that it displays the contents those are changed frequently or dynamically, for example, electronic score board or flight information displaying board. In general, a computer is employed for this second type of display-board. However, in this case, the computer should be always busy, even if for displaying a fixed content, engagements for sending data continuously to one column-LED after another of the LED-array in order to display any information. Therefore, it will hardly be possible to have the computer free to do any other job. In addition to this, to provide this type of electronic display board at low cost is a great industrial challenge in these days. From this viewpoint, in this work, a system has been developed for a PC controlled electronic display board by employing a low cost old-dated 386 series computer and necessary software has been developed too to drive that system. The main features of the system are, it uses software controlled synchronous serial data communication between PC and display-unit, in the display-unit, there is also a memory subsystem which holds the information that are received from the PC for displaying, for displaying that information there is also a local controller which controls displaying mode whatever it is still or moving text or image and finally this system can work independently without help of PC. This software is capable of controlling still or moving text or images.

II. DESIGN CONSIDERATION

The block diagram of the proposed hardware is shown in Fig. 1. The design part of main hardware is divided into the following sub-circuits:

A. PC Interface circuit,
B. Serial to Parallel converter circuit,
C. Memory sub system,
D. Display unit circuit,
E. Device control circuit.

A. PC Interface circuit

The interfacing circuit [2~5] can interface between the display board and PC. Following the address decoding part, this circuit accepts lines from PC: one data line, one clock pulse line and another common ground line. The computer program can transmit data via data line serially along with programmed-clock pulse for every single data bit.

B. Serial to Parallel ConverterCcircuit

The serial to parallel converter circuit converts the serial data come from the computer into parallel format. The data is shifted into the sift register (SR) at every clock pulse, at the same time, the clock line is fed to a counter via an inverter. This causes a half cycle delay between data shifting in shift register and counting the counter. This was done in order to prevent the loss of data. When 8 bit data are shifted into the shift register completely, at that time the counter value is 7. At

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

this time the temporary data register (TDR), which is connected to the parallel output of the shift register, is enabled by the counter, thus the contents of the shift register are loaded in the TDR as parallel data. Only this data will be available in the data bus of the designed system. The next byte serial data in the shift register will be available to a 3-to-8-line decoder (DR) through a tri-state buffer when the terminal count occurs in the counter. The second byte data is used for addressing various register/tri-state buffer and generates various control signals in the designed system for data-load operations or data-transfer operations. So, there are two bytes data are necessary for loading or transferring in parallel form. For example,

1st byte	2nd byte	Equivalent operation
XXH	00H	Load device control register (DCR)
XXH	02H	Load last count register (LCR)
XXH	03H	Load memory address register (MAR)
XXH	04H	Load memory via data line (MDR)

C. Memory Subsystem Unit

The memory subsystem consists of a 2048X8 bits memory package 6116 [6] for storing data that will be displayed to the LED monitor. A local control-circuit places the proper address at Memory Address Register (MAR) that should contain the data to be displayed on the LED monitor; in this way desired portion of the memory can be selected for displaying data. Therefore, the function of the local controller is to read the appropriate column-data of the LED monitor as well as to control whatever the contents for displaying should be static or moving.

This local controller consists of a counter, comparator and register. However, during this write operation that local controller is disabled. For memory-write operation, at first, the address is sent and following that data is sent. After write operation the MAR and the memory buffer (MB) is disabled and the local controller is enabled by the device control register.

If the content column-data are equal or less than the number of columns of display units then the contents are displayed on the monitor will be static or still. In this case, after displaying a complete set of data, again data-reading should be stared from same initial memory location. In order to display moving contents, two set of same data are stored consecutively, .and starting memory location for read operation is shifted one step advance or back after finishing of displaying one set of data.

D. Display Unit Circuit

The display unit circuit has been built with 8X16 LEDs. The row LEDs are connected commonly for data that are available for any column. The column LEDs are connected commonly for displaying the data of a selected column. The column data are primarily stored in a latch and a 1-to-16-line decoder selects the desired column. The column decoder uses decoding by a counter, which counts continually with the clock pulse comes form the main circuit.

E. Device control circuit

The system has a control register, which can be used to control the device. The control word of the status register is shown in figure-2.

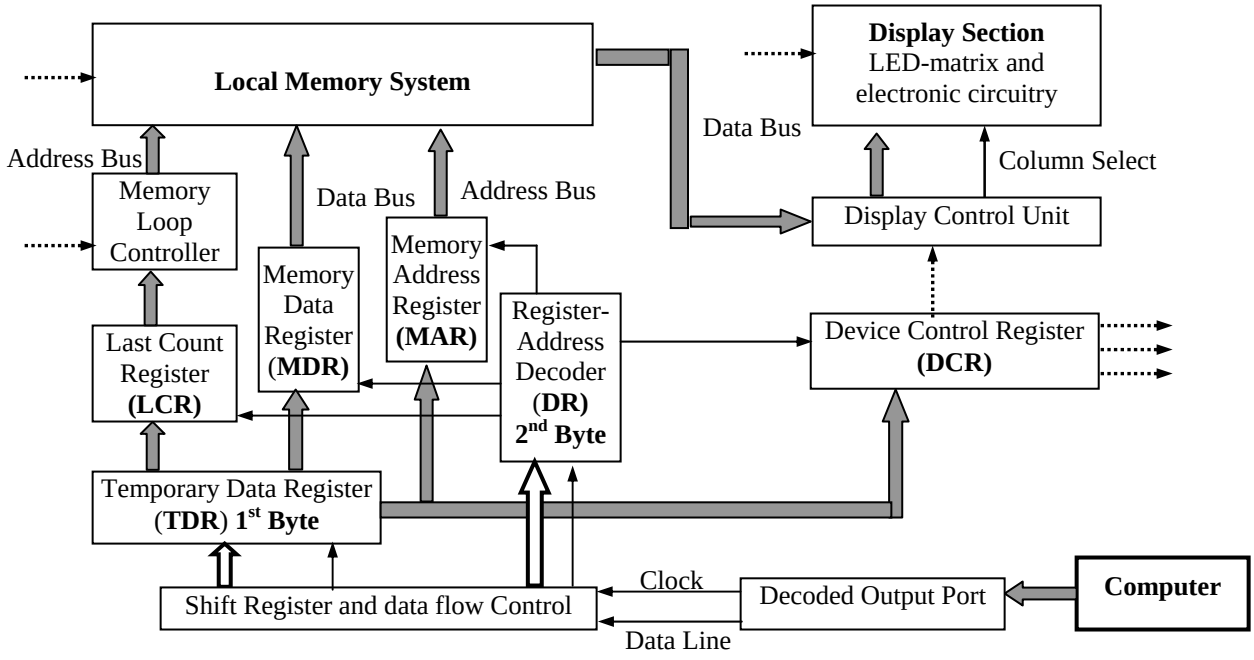


Figure 1. Block diagram of PC-controlled electronic display board

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The D_0 bit can be used for switching to clock pulse line. The D_1 bit can be used to enable or disable the address lines and counter lines. The D_2 bit is used to turn on or turn off the data sending line for the display unit.

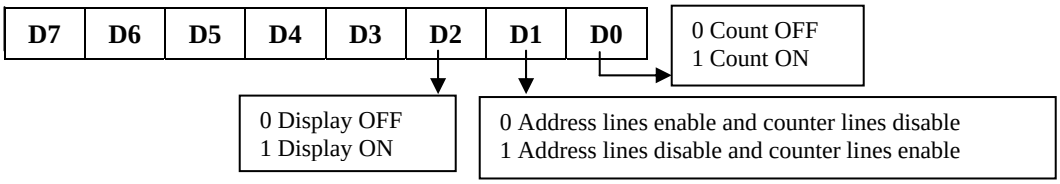


Figure .2. Device control word

III. SOFTWARE DESIGN

The program of the device, that can control its all operation, is written in C [7] programming language. The algorithm is given below.

A. Program Algorithm

All characters are formatted by 8X8 matrix of square array. For example character 'A' has the following format. All 0's represent no power present and all 1's represent that power supply is present.

```
A = { 0 1 1 1 1 1 1 0
      1 0 0 0 0 0 0 1
      1 0 0 0 0 0 0 1
      1 0 0 0 0 0 0 1
      1 1 1 1 1 1 1 1
      1 0 0 0 0 0 0 1
      1 0 0 0 0 0 0 1
      1 0 0 0 0 0 0 1 };
```

Therefore, the column values are sent one after another to the LED-array so that it looks like 'A'. In this way all characters and any other picture or images can be formatted compatible for this system. The program takes the value of each column and represents its corresponding integer value and transmits the value to store in the memory of the memory sub-system. Then, the device an display the contents of the memory according to its data values. The flow chart of the software is shown in Fig. 3.

IV. CONCLUSION

The project has been developed to show something in large-view. The total cost of this hardware is about 12 USD, this design involves some old-dated computers those are unusable otherwise, but those will have some industrial value. Therefore this low-cost displaying system can be sued as information displaying at different rail-station, airport etc, particularly for third world countries.

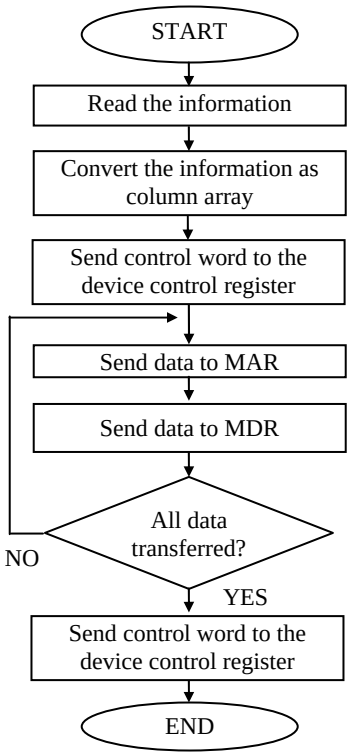


Figure 3. Flow cart of the program.

REFERNCES

[1]. J. Millman, C. Halkias, Electronic Devices and Circuits, TATA McGraw-Hill Edition, 1994.

[2]. H. Guang, Y. Yunyang, "Electronic display Board Monolithic computer", J. of Electron Devices, vol 1, 1998, www.cnki.com. cn

[3]. D. V. Hall, Microprocessors and Interfacing: Programming and Hardware, TATA McGraw-Hill Edition, 1991.

[4]. W.A. Triebel, A.Singh, The 8088 and 8086 Microprocessors: Programming, Interfacing, Software, Hardware, And Applications, Prentice-Hall of India-2002.

[5]. M. Rafiquzzaman, Microprocessors: Theory And Applications- Intel And Motorola, Revised Edition, Prentice-Hall of India-2002.

[6]. R. J. Tocci, Digital Systems: Principles And Applications, Sixth Edition, Prentice-Hall of India-1996

[7]. Microprocessor Data Hand Book, BPB Publications.

[7]. H. Schildt, Turbo C/C++: The Complete Reference, Second Edition

http://sites.google.com/site/ijcsis/
ISSN 1947-5500



M Gazi Golam Faruque: Received his BSc (Hons) and MSc degree in Computer Science and Technology from Rajshahi University, Bangladesh. Later he did M.Sc Engg. In Information and Communication Technology from Bangladesh University of Engineering and Technology. Currently he is working as lecturer, in the Department of. Computer Science Najran University, Najran, KSA He was the programmer of Bangladesh computer Council. His interested area of research is Embedded System Design.



Dr. Shamim Ahmad: Received his Doctor of Engineering in Electrical Engineering from Chubu university, Japan. He got his B.Sc (Hons) and MSc degree in Applied Physics and Electronic Engineering from Rajshahi University, Bangladesh. Following that he worked as research student in the department of Computer Engineering, Inha University, South Korea. Currently he is working as Associate Professor in the department of Computer Engineering of Rajshahi University. He was the former head of that department. His interested areas of research are Embedded System and Image Processing

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

An Approach be Operational Security in 3 and 4 Phases of Developing Software Systems

Saman Aleshi
Dept. Department of Electrical and Computer
Islamic Azad University, Zanjan Branch
Zanjan, Iran
SamanAleshi@gmail.com

Nasser Modiri
Dept. Department of Electrical and Computer
Islamic Azad University, Zanjan Branch
Zanjan, Iran
NasserModiri@Yahoo.com

Hossein Fruzi
Dept. Department of Electrical and Computer
Islamic Azad University, Zanjan Branch
Zanjan, Iran
hforouzi@gmail.com

Abstract— **Security in today's software applications because raw data acquisition system at the lowest level, the position is very important however, part of the development application under consideration is the security and therefore also delirium costs have to using and user. Security is essential in software development because the resource is protected to the integrity, availability and privacy of data guarantee. There are different models and standards for information security. PSSS is one of those models specialized for providing security tasks in PSSS, as an efficient software security model, in order to map in along with other security models and standard for 3 and 4 phases of software development, ensuring safety of task performance in the phases.**

Keywords - IT (Information Technology), IT security, Security Models and Standards and their limitations.

I. INTRODUCTION

Information which can be in various forms is the great asset an organization or business owns and is of vital importance, like other assets. Because it is shared among the parts of an organization or business, it causes great concern. Therefore, it needs ways for protection. In particular, in environments where business interactions are growing and data are shared it assumes great importance. Thus, the increased information dissemination subjects the information to a variety of threats and damages [20].

Progresses in the field of IT and communications and innovations resulting from it have increased productivity and lead to emergence of new types of services. With the improved ever increasing power, capacity and price of micro electronic equipment which have led to the about 30 percent make it possible for all people to take advantage of this technology. Today we live in a communication costs are falling.

And, the world people increasingly exchanging and information and communication systems, attacks and threats against such systems have increased as well. Security is considered as one of the key issues raised while developing the systems [2]. The number of these attacks are so high that, over the past years, more than 3500 annual damages have been reported to Computer Emergency Readiness Team/ Coordination Center (CERT/CC) also, around 140000 security events were presented to the center. The events happened were so great that CERT stopped publishing the statistics in 2004. The U.S Department of Defense announced that the number of computers with security gaps 88% and 96% of these computers however are not aware of this defect [18].consequently IT will play a major role inhuman life if its security is provided. Failures in IT security result not only in destroying its enormous benefits but also in changing into a life threatening factor [10].

IT is made up of various sectors such as human resource, hardware, software, data, equipment and communication protocols, electronic and electric devices and so on. Dealing with all of the sectors is beyond the scope of this paper. We will focus on application software.

Security like reliability or efficiency is one of the non-functional properties of the system. IT defines one of the attributes of the system which reflects its capability to protect itself against intentional a or unintentional external attacks, hide the nature of information or resources, Prevent unauthorized access to disclose private information; and data and resource reliability [7].

Security is defined as the situation in which a person is proceed from risks, threats and damages coming from social life. Security is a fundamental, relative and stable need which according to different view, can be to different extent and degree. In principle it is hard to identify, evaluate and implement security in a system [20]. According to Devanbu security, like beauty, is in the eye of the beholder [11].

Information security is the protection of information against a wide range of threats in order to ensure continuity of business, minimize business risks and investment opportunities. Information security is achieved by implementing a set of effective controls including policies, processes, procedures, organizational structures and software and hardware functions [1].

Security has access to data at the lowest level and shares them among user in various sectors. Sharing information, however, causes excessive concern in organizations because security and protection are the key elements of sharing data. Applications can have a lot of gaps in different sectors [13]. Less experienced programmers, software at the risk of abuse, unskilled individuals lacking necessary skills or resources for testing software are some of the reasons that have increased the number of gaps [12]. That's why security, especially for

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

large organizations and corporations with data of critical importance has caused concern. On the other hand, software users and developers are mostly businessmen, not professionals. Therefore information security is not of concern to them and they overlook it [3].

Secure software is software that cannot be forced to perform unwanted tasks. Security at software can be considered from two perspectives. First perspective relates to development of the software and creation of a safe environment to keep it. The second perspective is about the development of software itself in a safe manner. Therefore, security is considered at different phases of software development [17].

Software development is composed of the following phases [22]:

- **Initial Phase**: during this phase, all the necessary requirements for design or purchase of the system are determined and fully understood.

- **Development/Acquisition Phase**: In this phase, functional and technical needs are mapped into information system programs.

- **Implementation/Assessment Phases**: In this stage, all tasks performed in analysis and design phases are mapped into readable codes for computer by developers and programmers.

- **Operation/Maintenance Phases**; this stage, involves all activities required to keep the system functions in good condition; these activities include wpkeeping the hardware and reducing application faults.

- **Disposal phase:** In this stage, the system is replaced by another one or its feature is not needed any more.

There are several models used to create information or software security. In this paper we aim to map one of these models specialized in creating security for software and giving better results in comparison with other models and standards-into software development phase; accordingly the software safety would be acceptable after it is created.

The activities that will be done in this paper are as follows: section II deals with measures taken in the field of software and information security and limitation of those measures. In the III section considering the current models and standards the reason for which the issue of security is reconsidered is presented. The proposed framework is presented in section IV. The tasks that need to be perfumed in the third and fourth phases of software development are given in sections V and VI results and conclusion of the study will be give in section VII and the references in the last section.

II. COMPLETED TASKS

Tasks performed to create security for software and information will be summarized below.

- **Security System Engineering – Capability Maturity Model (SSE-CMM):** a reference model is a process of providing a comprehensive framework for evaluating security engineering activities to concentrate requirement for implementing of IT security. Different models and standards such as GMITS, NIST HANDBOOK, and BS7799 are derived from this model [14].
- **ISO/IEC 27002:** this standard provides guidelines and general principles of starting, running, maintaining and improving information security management in an organization. Control objectives and controls considered in this standard to meet the needs identified in risk to developing organizational security standards and to effective security management practices in order to make inter-organizational activities reliable [1].
- **Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Model**: this model focuses on the risk analysis of information technology assets and practical solutions for reducing risk factors through overcoming discovered security flaws. OCTAVE is designed for organizations that want identify what their information needs to be secure [19].
- **ISO/IEC 15408:** this standard having considered the results of security assessment, this standards permit comparison. To do so it prepares a set of requirements for security function of IT products and system. And its standard ensures their use according to security assessment.[16]
- **Team Software Process-security (TSP-Security) Model**: This is one of the specialized models focusing on software security. Software Engineering Institute (SEI) and Team Software Process (TSP) are a set of operational process for use by software development teams. TSP is a set of processes t help develop software. It also shows how to do things step by step and how to assess the completed task. To create security while developing software, SEI has added issues related to the security of software development cycle to TSP [9].
- **Process to Support** Software Security (PSSS) Models: Process to Support Software Security (PSSS), as a perspective on security engineering is associated with software development. This relation aims to improve the efficiency of security projects by means of a set of activities in aforementioned models and standards; accordingly developing and organizing behaviors at time of software development, it deals with common problems and limitations of information security model [21].

PSSS has two important parts: Security Engineering and Security Auditing. Based on the goals followed by software development, security engineering is to establish contact with business plans and strategies, to monitor project in order to archive security goals. Security audit is responsible for ensuring whether software development is in compliance with PSSS or not.

This individual verity the impact of PSSS programs. For example, they state the results of activities and achievements in certain circumstances. A series of activities that should be done in PSSS are as follows:

- Planning security
- Assessing Security Vulnerability
- Security risk model

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- The impact of risk assessment
- Identifying security risks
- Specifying security needs
- Providing security information
- Verifying and validating security
- Managing security
- Monitoring security behavior
- Ensuring security

Other standards can be added to these models and standards in the field of information security. In addition to models and standards used in the field of information security, there are other pieces of software such as firewall, Intrusion Detection Protect (IDS) or other applications like them that protected software data after it is created. Simply put, they enhance software security [15].

But it still isn't easy to use these models and standards for the following reasons [21]:

- **The limitation of SSE-CMM**: it is a complicated model because it does not perform all tasks the system needs. Furthermore it does not explain how to perform the processes in the areas mentioned. Thus, it is hard to apply and implement this model.
- **The limitation of ISO/IEC 27002**: it includes a large number of security controls executed in different processes of various organizations. Also, it does not demonstrate how to execute security control in the best way, not specifying a standard.
- **The limitation of OCTAVE**: It tasks a self-directed approach. Simply put, an individual from the organization assumes responsibility for setting up, implementing and controlling security.
- **The limitation of ISO/IEC 15408**: Due to its complex relationship which entails specialized knowledge, it is costly and time consuming. Moreover, it focuses only on certain software products and overlooks the interrelationship between other software products.
- **The limitation of TSP-Security**: First of all, its use requires investment in training and software developers should have necessary training for using this model. Accordingly, the TSP use demands senior and project manager's support. Besides, for most organization, effective TSP use requires that the management and technical culture and character be able to perform technical tasks carefully and consistently, the leadership be sustained, be a driving force behind making TSP team self-directed.
- **The limitation of PSSS**: Identification and understanding software property, lack of specialized knowledge for functionality in all activities associated with threat model and need for more resources necessary for effective PSSS function.

III. CRUCIAL IMPORTANCE OF SECURITY

In addition to limitation and problems that were described above for the models and standards, here, we will discuss the problems demanding that security be considered all the time, though there are models and standards for this purpose.

A. Software Security needs a serious consideration

- The losses suffered by countries, companies and organization for software intrusion and damage are too costly. For one thing, the additional costs for U.S. government potential attacks on critical infrastructure remain a serious concern. New automatic attack requires no human action to deliver4 destructive play loads, causing major concerns. In 2004 over 140000 attacks were reported to CERT which is due to holes in software and networks from 1999 to 2003(see figure 1).

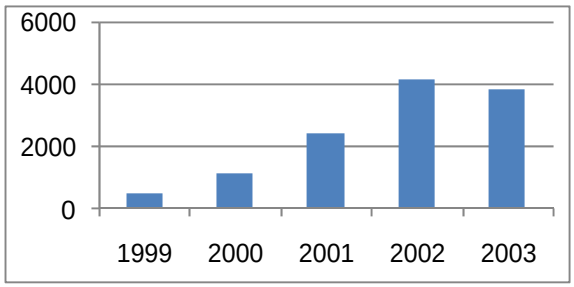


Figure 1: Holes reported by CERT CC

- security holes, if any, can have adverse effects on software, e.g. , negative effect on the reliability

B. To develop security software is complex

- Computer science is very extensive. For instance when you combine two or more parts of a software to each has certain security characteristics the combined results should not demonstrate security characteristics. To do so you need careful analyses.

- When developing software with high quality, you need educated and experienced personnel.

C. It's hard to define secure software in general

- The first necessity for software to be safe is defining necessary specifications and properties. Security, it is necessary to implement the specifications accurately.
- What kind of security and privacy are required, what are its costs and risk? These questions are hard to answer; technical judgment does not help. Because it requires you to view it from management and marketing perspective. In particular, when customers don't have great interest in it or they have to pay for it, such view can be helpful.
- Finally, developing software with the qualities of privacy, integration and appropriate accessibility which entails the above-mentioned problems has made defining a security software challenging.

D. Why are not the existing approaches in wide use?

- Cost and needs are among the greatest hurdles in the way of an organization which cause concerns when creating security software, though there exits other reasons such as users comfort, quick supply, more functionality and so on.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- After the customers and users awareness increased, security was in great demand. But it's not paying the costs of security.
- According to Microsoft reports, 20% of the security faults are due to its design. To avoid such issues specialized skill and knowledge for security and design are required.

IV. PROPOSED FRAMEWORK

In comparison with the methods and standards for software products security, as PSSS focuses on security in a specialized manner, it has particular importance. And because it has produced satisfactory results, in parts put into use PSSS has attracted importance. Other methods and have rudimentary conceptual foundation and don't put much emphasis on designing and analyzing phases, not producing the same results as PSSS. However, PSSS has its own disadvantages that were mentioned above [5].

Software development cycle has phases which the input of each phase is the output of previous phase. So, if we can deal with security issues in each phase besides software development, it is possible to produce secure software. In each phase, there are criteria and parameters associated with security which should be met; otherwise transition to next phase will be impossible. According, after the software development phases have been completed, the product will be secure software.

In this paper, security tasks mentioned id [21] along with other security issues associated security models and standards are divided into groups. Phases of software development are show in [22]. Grouped tasks are so that tasks of each group are consistent with one of the phases of software development. In fact, each group contains a set of security tasks that should be done in a phase of software development. Each of these along with a set of tasks necessary for software development is described and continued. Finally, after the end of each phase, the product is compared against security standards. If security is acceptable, we will enter the next phase. This procedure is followed in the other phases. On the other hand, if the product isn't security measures will be tightened.

Besides the things that to establish security in software are described, Output that each task security must have, Work independently parallel to the security task, And work-related security tasks that must be done to increase security in this article is also shown. Figure 2 is as a schematic of tasks that to be done, show in this paper

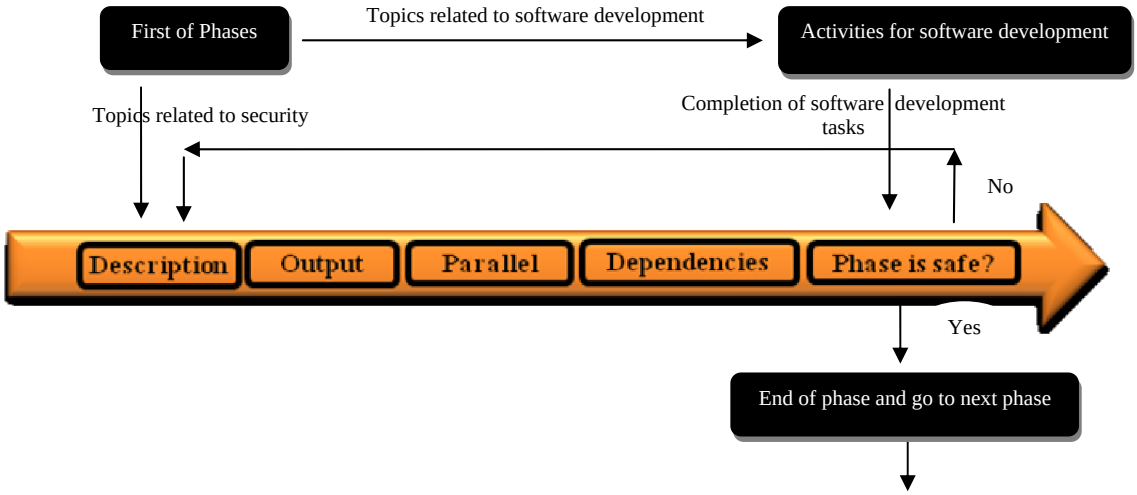


Figure2. The Proposal Framework

This paper describes activities to tighten software security-besides; the output of these activities, activities dependent on and independent from these security activities are also included in the paper.

- **The initial phase**: at this stage in the project, how to initiate the activities are demonstrated
- **Software development activities**: activities and tasks performed to develop software.
- **Description**: activities and tasks to tighten security are identifies and described.
- **Output**: the result of activities done are demonstrated which creates a situation to elicit proposals and comments on the past and future activities.
- **Synchronization**: activities that should be performed at the same time with those to tighten security are necessary.
- **Interdependence**: key interdependence besides other necessary tasks is identified to make sure that coordinating security activities have no negative effect on other processes of IT.
- **In phase safe**?: The situation is reviewed to see whether the software has lived up to the expectations or not.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- **End of the phase and going into next phase**: at this stage, the software is developed safely and it can enter into the next phase.

In next section, we present the tasks should be performed in the first, second, third, fourth and fifth phase according to framework offered in the present section. Accordingly when we complete a phase, it can enter into the next phase safely.

V. THIRD PHASE OF SOFTWARE DEVELOPMENT, IMPLEMENTATION/ASSESSMENT PHASE

Necessary tasks of the phase are as follows:

A. Creating a detailed plan for C&A

a. **Description**

AO is responsible for risks to the system. There is a relation between risks and final operation of the system. If there are undetected risks to the system, they can cost an arm and leg to the system later. There for, AO is required until the risks are fully identified. Combining changes needed during the planning stage as required, risk identification makes it easy a simple to select resource.

AO and development team should cooperate in: solving problems relating to test results and data in the system; how the changes should be made; how these changes should be reflected in the environment; and how a secure working group working – that can include people such as users, managers, plan supporting , administrational including A&C, and system analyzer- can be formed.

b. **Output**

Initial work plan: planned documents identify key roles, project limitations, main parts scope of the test, and a degree of accuracy.

c. **Synchronization**

Informing AO about the things, ISSO system owner's complete and present documents required C&A initiation and conduct.

d. **Interdependence**

Planning for assessment of security controls extracts necessary information from documents or scheduled meeting.

B. Integration of security into the system or established environment

a. **Description**

Operation integration tasks place at the operational site when information systems are expanded for an operation. After information systems are delivered and installed, integration and acceptance testing occur. When security controls are included in the developer's instructions, guidelines will be available for implementing security, offering documented security specifications.

b. **Output**

- Verification of a list of operations of security controls.
- Completion of system documents.

c. **Synchronization**

- Issues arising during the installation should be evaluated for inclusion into contingency plans based on the potential for reoccurrence.
- During the system installation ISSO should make sure that controls are located in place and configured properly and deliver the verified list to the system owner and AO.

d. **Interdependence**

Changes to the core security documents should be updated.

C. Assessment of system security

a. **Description**

System development or changes in hardware, software, or how they interact must be validated before evaluation. The purpose of security assessment processes is to validate that the system is consistent with functional and security requirements and it has an acceptable level of security risk. Security controls should be done. Before the initial operation, security endorsement should be issued to the extent controls are implemented, operations are confidence. Finally, the desired results are achieved and evaluated. Also, periodic testing and assessment of security controls in information ensure efficiency of security controls, security validation may discover and describe gaps in the information system. With efficiency of security controls and information system gaps made clear, we have essential information for authorities to issue permits necessary to fill the gaps.

b. **Output**

Security assessment packs include reports for security assessment, POA&M and updating system security plans.

c. **Synchronization**

Results of validation packs are issued in written form for owners of the system, ISSO and system administrators and assessment results are shared among them.

d. **Interdependence**

All previous steps are followed.

D. Authorizing information systems

a. **Description**

To process, save and transfer information security authorization of security systems are required, these permissions issued by security authorities are to state that security controls are checked. Decision on security certificates is risky and it is heavily dependent on testing results and security assessment produced during processes of security control verification licenses are as allows:

- To complete system security plans
- The results of testing and security assessment
- POA&M

b. **Output**

- Authorized security decisions will be documented and transferred from authorizing officials to system owner and ISSO.
- Final security authorization package

c. **Synchronization**

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- Statistics for inventory and reports of the system should be updated to reflect a valid condition.
- If the system is valid, CPIC activities will be reflected

d. **Interdependence**

- Security documentation and budget are updated according to the results.
- The structure of information systems is validated.

VI. Fourth phase of software development, Operation/Maintenance Phase

Tasks necessary for tightening security in this phase will be presented below:

A. Review of operational readiness

a. **Description**

In many cases that systems are transferred to production environment, unplanned changes are drastic, security controls are modified or integrated although these steps may not be always required, they can reduce risks, if any.

b. **Output**

If there are changes in the system, the implications for security are examined.

c. **Synchronization**

System administrator and ISSO and the owner of system confirm that system operations are consistent with security needs. Changes observe at the last moment are dangerous for the system and should be verified by the system owner.

d. **Interdependence**

- Review of operational readiness which is complement to C&A processes ensures that the changes already made will eliminate potential risks.
- Any changes in security controls should be reflected in security documentation.

B. Control and management of the configuration performed

a. **Description**

Efficiency of management control of the organizations configuration and reflected methods are necessary in order to take security impact into due consideration with regard to changes in information systems or their surrounding environment. Management and configuration control methods provide initial baseline for hardware, software or programs which are always in the memory. This baseline is essential to information systems. Subsequent changes in the system will be controlled and maintained.

Documentation of changes in information systems and assessment will have a major effect on maintenance of the validation. When important and essential inputs are combined with be followed effectively. According, the ability of an organization to identify considerable changes facilitates the control of system security and the impact of security. This helps to make sure of assessment and testing.

b. **Output**

- Decisions of Change Control Board (CCB)
- Updated security documentation (System security plan and POA&M)
- Security assessment of documentation changed in the system.

c. **Synchronization**

- Security documentation should be updated at least once year become of the marked changes.
- CM documentation should provide continuous monitoring plan for the system.

d. **Interdependence**

Security architecture should provide key details of security services to components which is used as a criterion for effective evaluation of planned changes

C. Monitoring the results continuously

a. **Description**

The ultimate goal is continuous monitoring. It guarantees effective monitoring when there are inevitable cases needing security control. Good management and design of continuous monitoring processes can lead to reduction of risks effectively by meeting all of the requirement. Monitoring the efficiency of security controls continuously can be done using various methods such as security check, self-assessment, configuration management and security assessment and testing

b. **Output**

- Results of documented continuous monitoring
- Review of POA&M
- Security review, metrics, assessments, security analysis trend.
- Updating security documentation and decision on validation.

c. **Synchronization**

Continuous monitoring should be regulated so that the risk level may become lower significantly. Therefore, security controls are changed, increased or discontinued.

d. **Interdependence**

Continuous monitoring enables system owners to update reports of security assessment; they use a right tool for monitoring the products continuously which is based on the security plans of information systems.

VII. Result and Conclusion

Activities stated in this paper were done to design, implement and execute software for management of a “three-star HOTEL”. Results achieved for implementing the software and using the tasks suggested in the paper are summarized below:

- Raising awareness of importance of security in software development, using a self-oriented process, based on well-known security methods.
- It has been defined as a factor of the assessment and evaluation of vulnerability, threat, impact and security risk in each phase of software development based on security measures.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- Showing the importance and necessary of the assessment necessary to security , based on vulnerability, threat, the impact on and security risk to information;
- Emphasize on importance of security tests, as a criterion for assessment and approval of security, is a permanent and continuous activity which depends on verification of security requirements.
- It states a need for formal definition of processes to ensure that the established security acceptable.

In the end, we want to review what have been done in this paper. In first section, the reasons for the interest in the security were offered. What have been done in this regard and the limitations were stated in second section. In third section, we stated that considering available models and standards, security should be given more attention. In fourth section, we suggested a framework that we want to map PSSS into phases of software development with this framework. PSSS is specialized in development secure software. Section V and VI presented the tasks that should be performed within the proposed framework for 5phase software development. The results of action within this framework to produce the software for the management of 3-star hotel are presented in section 10.

REFERENCE

[1] Iranian national institute for industrial research, 2007, IT-security techniques- Information security management Function, Tehran, iran, 1st volume

[2] extension of RUP for development of secure system, Hamidreza baghi, Puya Jaferian, gholnaz sadeghian, computer engineering and IT school, Amir kabir technical university, annual conference of Iranian computer sociery 2004.

[3] security measures for non-agent defence in IT environment, MA thesis, higher Education school, Tehran jonob Azad university 2009.

[4] a framework assessment of detect and gaps in software application, Esmat Ali Mohammad, MA thesis, higher Education school, Tehran shomal Aazad university, 2009

[5] Security software architecture engineering, Nasser Modiri, mehreghan-e-Ghalam publication, Tehran, Iran, 1st volume

[6] Noopur Davis, Michael Howard, Watts Humphrey, 2004, "Processes to Produce Secure Software", National Cyber Security, Volume 1

[7] Al Azzazi Ahmad, El Sheikh Asim, "Security Software Engineering: Do it the right way", Conf. on Software Engineering, Parallel and Distributed Systems, 2007, 6th, 5.

[8] *Joint endeavor by* Information Assurance Technology Analysis Center (IATAC) with Data and Analysis Center for Software (DACS), 2007, Software Security Assurance State-of-the-Art Report (SOAR), Woodland Park Road, First Publication.

[9] Watts S. Humphrey, *November 2000*, the Team Software Process (TSP), Carnegie Mellon University – USA, 1

[10]A.Kumar,K.Negrat,A.M. Negrat,and A.Almarimi," A Robust Watermarking using Blind Source Separation", Proceedings of world academy of science, engineering and technology ,vol.28,April 2008.

[11] Barnum, S.; McGraw, G., "Knowledge for software security", Security & Privacy IEEE, March-April 2005, Volume: 3, Issue: 2,

[12] Gilliam, D.P, "Security Risks: Management and Mitigation in the Software life cycle", IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'04), 2005, 13th, 6

[13] Yasar, A.-U.-H.; Preuveneers, D.; Berbers, Y.; Bhatti, G.; "Reported flaws in Common Vulnerabilities and Exposures Database", Multitopic Conference, 2008. INMIC 2008. IEEE International, Dec 2008, 11,

[14] Hopkinson John P. "the Relationship between the SSE-CMM and IT Security Guidance Documentation", Principal Engineer, Security Architect EWA, 1999, 18

[15] David Gilliam, John Powell, Eric Haugh, Matt Bishop, "Addressing Software Security and Mitigation in the Life Cycle" Software Engineering Workshop, 2003. Proceedings. 28th Annual NASA, 8494821, Page 201 – 206

[16] Zeinab Moghbel, Nasser Modiri, ,"A Framework for Identifying Software Vulnerabilities within SDLC Phases", (IJCSIS) International Journal of Computer Science and Information Security, 2010, vol 9

[17] James E. Purcell, "Defining and Understanding Security in the Software Development Life Cycle", 2007

[18] www.sse-cmm.org/ *last visit: September 201*1

*[19]www.cert.org/octave/ last visit: September 201*1

.[20] Gilbert, Chris, 2003 11, Guidelines for an Information Sharing Policy, SANS Institute - USA, version 1

[21] Francisco José Barreto Nunes1, Arnaldo Dias Belchior, "PSSS - Process to Support Software Security", XXII Simpósio Brasileiro de Engenharia de Software. Oct 2008, 4th.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Analysis & Selection of Requirements Elicitation Techniques for OSSD

Munazza Ishtiaq[#1], Fareeha Choudhry[#2], Fahim Ashraf Awan[#3], Aasia Khanum[#4]

[#1, 2, 3, 4] *Department of Computer Engineering, College of Electrical & Mechanical Engineering*

National University of Sciences and Technology (NUST)

Rawalpindi, Pakistan

[1]munazza.ishtiaq@gmail.com

[2]fareeha.choudhry@seecs.edu.pk

[3]fahimawan18@yahoo.com

[4]aasia@ceme.nust.edu.pk

***Abstract* — Open Source Software development (OSSD) is unlike traditional software development in many aspects. Requirements elicitation is the most critical phase in software development as it is the basis for developing software. The requirements elicitation phase in OSSD is different from traditional software development process and somehow a difficult process as the developer is the only person that has to elicit the requirements and then make the software open for review from the user community. The users can add or modify the product according to their own needs and requirements. The focus of this paper is on the requirements elicitation phase and elicitation techniques for open source software development. In this paper, requirements elicitation phase model for OSSD is proposed as well as best suited requirements elicitation techniques for OSSD are discussed and a framework for choosing and comparing these techniques is developed and the selected techniques for OSS are analyzed in the context of the criteria mentioned in the framework. A formula is proposed using the framework and the proposed model for the requirements elicitation process and selection of techniques for OSSD.**

***Keywords* — framework, OSSD, requirements elicitation process model, requirements elicitation techniques, traditional software development**

I. INTRODUCTION

Open source software development refers to a program or software in which programmers develop software and make it available to public for studying, modifying or changing the code under an open source software license agreement. In this way the code is being improved by the public and becomes more error free as well as quality of software also gets better, then these changes are again shared with the public [1]. Open source software can be developed when there is a need for that software but its requirements are not clear or there is a room for software improvement, so the developer develops software with some limited functionality and makes it public for the community to use it and modify the code to improve software or add functionality to it. For developing a software product the first step should be planning about what is to be developed and how it is to be developed. The next and most critical step in software development is requirements elicitation. Requirements elicitation is done to gather the requirements by interacting with the customers or system users for developing a project. It is the most vital phase of software development. Requirements elicitation provides a developer with complete and consistent set of requirements through which he/she can develop the project. Many methods have been proposed for requirements elicitation but still there is a need to develop a more comprehensive and stable method to develop a quality product. For OSS development requirements elicitation phase is carried out by the developers themselves because the users of the product to be developed are not known at that time. Even if OSS is developed for some projected community, it is complex to gather requirements from the whole community. For OSS, requirements continue to evolve as community members discuss and then reveal what they exactly want [2]. There is a need to understand how to select a technique for gathering requirements for open source software projects. This paper discusses the criteria for selecting an elicitation technique for OSSD by defining a criteria framework and analyzes each technique in the light of these criteria to judge which

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

technique is most appropriate for OSSD. This paper also presents a rule for elicitation technique selection using the criteria discussed in framework and the proposed model for requirements elicitation process for OSSD to provide the OSS developers a better understanding of each technique as well as to help them choose an appropriate technique for their project.

The organization of the paper is as follows: literature review is presented in Section II of the paper, section III describes a brief introduction of OSS and OSSD, section IV describes the difference between classical and OSS requirement engineering process, section V describes the proposed framework for the selection of elicitation techniques. Section VI presents selection of elicitation techniques for OSSD. Section VII explains the framework and proposed model in detail. Conclusion and Future work are provided in section VIII of the paper.

II. LITERATURE REVIEW

OSS development has proved itself to be an effective and flourishing development but the problem with this development is that there is no proper lifecycle model for building OSS products. The most important phase of OSSD is to gather requirements as the users of the OSS product are not known at the development time. The developer has to elicit the requirements by keeping in mind the users of the product. A lot of work has been done in OSS development field to study the requirements elicitation process. In [2] the author has studied different OSSD communities and has described that developing requirements for OSS is a community building process that must be done by keeping the users of a particular community in mind. The requirements for OSSD continue to evolve and the author has provided a framework that depicts how OSS and their relevant communities are interlinked with each other. One of the success factors of OSS products is that the developers of the product are the users of the product so they elicit the requirements according to their own needs and based on their deep understanding [10]. In [9] the authors have discussed that there is no proper documentation for OSS products instead the requirements are discussed over the Internet through emails or blogs. The requirements for OSSD are not elicited at the beginning of the project rather they are clarified as the development proceeds. A single developer thinks of an idea and starts the project based on his own experience [11]. In [3] the authors have presented several requirements elicitation techniques which can be helpful in OSSD which are: Discussion, introspection, questionnaire interview, protocol analysis, discourse analysis, open ended interviews.

III. WHAT IS OSSD & OSS?

OSSD stands for Open Source Software Development. It refers to such type of development in which the developers identifies a problem and tries to develop a product by eliciting requirements themselves and then developing the product. The product along with the source code is freely available for use by the public and they can modify the code, add functionality and use it or redistribute it according to some defined policies. Apache case study [8] has differentiated between OSS and commercial products. Differences are described below:

- OSS products are developed by volunteers not by professional developers.
- In OSSD tasks are not assigned to particular persons instead volunteers carry out the development.
- OSS does not have any design phase.
- In OSSD, there is no planning, time or cost scheduling nor any deliverables.

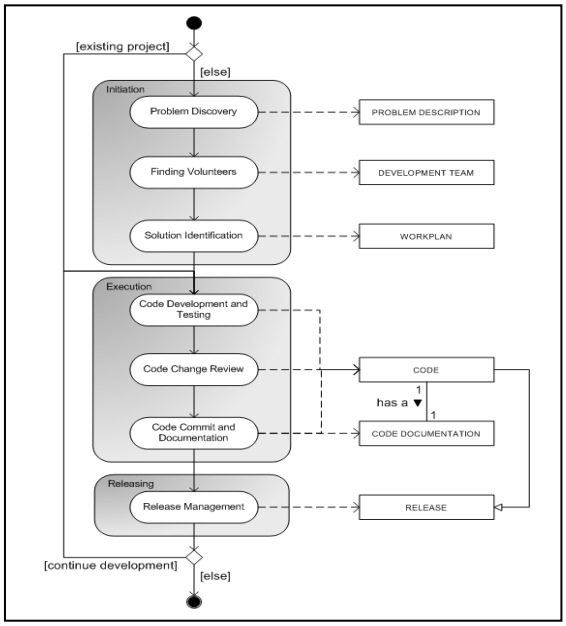


Figure 1: Life cycle model for OSS development (source: Wikipedia)

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Open Source Initiative (OSI) has identified several terms and standards that the open source software must fulfill [1]. These terms and standards are discussed below

1. Redistribution

OSS is freely available to everyone and it does not limit any one from redistributing it without any cost.

2. Free Source Code

The OSS program must contain the source code. If due to any reason the source code is not provided along with OSS, then it should be possible to get it from some authorized source.

3. Derived Work

The OSS source code should be freely available to everyone for variations in code as well as to add any required functionality. The product will be then available to the public under the same license agreement.

4. No discrimination against users

OSS must not discriminate among people. It is freely available to everyone and anyone can modify it and redistribute it according to the policies.

5. No discrimination against a specific field

OSS can be used in any field of study and there is no restriction of its use in commerce, business, and research or any other field.

6. Distribution of License

OSS license is distributed among its users so that they can make changes to the code, add functionality and then redistribute the code. Every person that contributes code to the OSS does it according to the policies described in the license.

IV. CLASSICAL VS. OSS REQUIREMENT ENGINEERING PROCESS

Requirements elicitation is defined as the process of gathering the requirements from the stakeholders or end users of the product. Fox C. defines the process of requirements elicitation as "the activity of determining stakeholder's needs and desires for a product" [13]. Open source software development (OSSD) process is unlike traditional software engineering development process. OSSD is carried out by some volunteers who find the need to develop some software and then make it public for the users to review and modify it. Whereas the traditional software development process is carried out by some professional developers and it is developed for some particular customers [12]. Therefore the requirements phase of OSSD and traditional software development also differs to some extent. Requirements phase is the most fundamental and complicated phase in software development, as stating what is needed becomes complex for the clients. Classical requirements engineering process includes Eliciting requirements, Modeling or specifying requirements, Analyzing requirements, Validating requirements, Communicating requirements [2]. For open source software development, requirements phase can be divided into sub phases which include requirements elicitation or more specifically it can be called as requirements assertion from the open source community using different techniques available, analyzing those requirements to remove duplicates, ambiguity and inconsistencies. After analyzing, requirements are again altered to maintain consistency among them and to include or exclude requirements; these requirements are then finalized.



Figure 2: Proposed Requirements Elicitation Phase in OSSD

Requirements elicitation phase in OSS development requires identifying the stakeholders of the product, their goals and expectations. For this purpose technique like introspection, questionnaires, discussions, open ended interviews are most suitable as they can be easily implemented but all these techniques have their own merits and demerits.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Open Source Software Development generally does not involve classical software requirement engineering process. Basic difference between the two approaches is that Classical Requirement Engineering process involves "Requirement Elicitation" whereas Open Source Software Development requirement engineering process involves "assertion of open software requirements" [2]

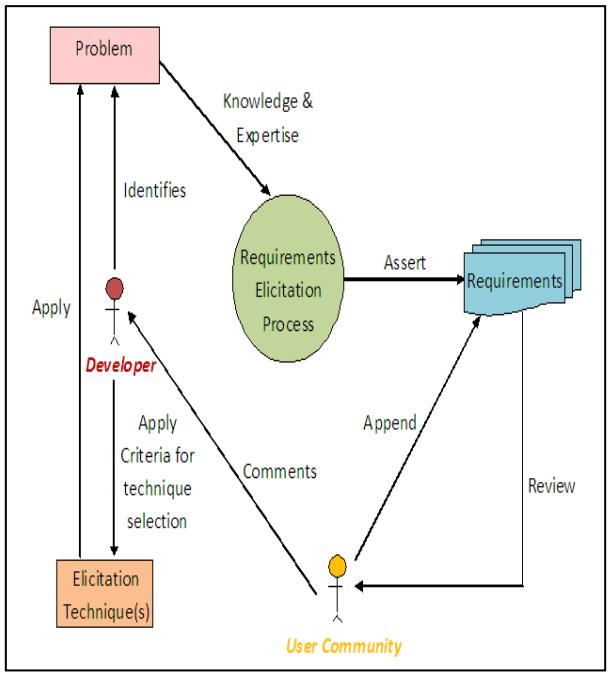


Figure 3: Proposed Model for Requirements Elicitation Process in OSSD

A. REQUIREMENTS ELICITATION MODEL FOR OSSD

This proposed model for requirements elicitation process of open source software development represents that the development process is mostly done by the developer of the product along with the review carried out by the users and their comments about the product. The developer may think of an idea to implement or identifies a problem. The problem is defined and requirements for that problem are elicited through the developer's experience and knowledge of the domain. To elicit the requirements further, the developer can apply the criteria defined in the framework below to select an elicitation technique. These requirements are passed on to the user community for review of the techniques so that they can also suggest new requirements or modify already elicited requirements in a better way.

The model can be understood by this formula for eliciting requirements:

If we have a problem say P_i, then it may be divided into further sub problem denoted by P_1, P_2, P_3… P_n.

$$P_i = \sum_{i=1}^{n} (P)$$

Requirements assertion (RA) can be performed by the developer through his knowledge about the problem domain as well as the expertise of the developer in that particular domain.

RA = Knowledge → Problem Domain ←Expertise

For eliciting the requirements to solve the identified problem these asserted requirements will also be analyzed to make them consistent and complete. The developer will study the elicitation techniques and will select a technique according to the criteria (C) defined in the framework and by evaluating the techniques according to some factors denoted by Ev in the formula such as effectiveness of the technique for eliciting requirements for the problem, resources required and end user involvement to select the best suited technique that consumes less resources and a small amount of end user involvement.

$Et = ((C_{i=1\ldots n} (T_1, T_2 \ldots T_n) \cap Ev(T_1, T_2 \ldots T_n), P)$

Or more specifically

$Et = (C(T_i) \cap Ev(T_i), P)$

Where {Et ϵ T | Et is applicable to some specific problem}

The elicitation technique(s) denoted by Et we get through the intersection of criteria applied to techniques and evaluating techniques according to the problem will be the set of the elicitation technique(s) suited for that specific problem.

$R_i = Et (P_i) \cup RA$ where $R_i = \{R_1, R_2 \ldots . R_n\}$

Set of requirements (R_i) can be gathered by applying the selected elicitation technique to the identified problem. The union of elicitation technique applied to the problem to elicit requirement and requirements asserted by the developer on the basis of acquaintance with the problem domain will be the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

final set of requirements. These set of requirements can be provided to user for review and suggestions.

V. FRAMEWORK FOR SELECTION OF ELICITATION TECHNIQUES IN OSS

A framework has been proposed in this paper based on the criteria mentioned in table 1 for the selection of requirements elicitation techniques and evaluation of each technique according to the criteria for open source software development. The notations used to express the techniques according to the criteria indicate following:

Notations	Meanings
+	Less Probable
++	Probable
+++	Highly Probable
-	Improbable

TABLE 1: Criteria Framework for selection of Elicitation Techniques for OSS

Criteria	Techniques			
	Introspection	Questionnaire	Discussion	Open ended Interviews
Adaptable	+++	++	+++	+
Usable	+++	+++	++	++
Ease of communication	++	+++	+++	+++
Understandable	++	+++	+++	+++
Implementable	+++	+++	++	+
Reflect stakeholder's goals	+	+	++	++
Remote Administration	+++	+	+++	+
Time Constraints	-	+++	+++	+++
Cost Free	+++	+	+	+

The framework is explained in detail with the help of an example in section VII**.**

VI. ELICITATION TECHNIQUES IN OPEN SOURCE SOFTWARE DEVELOPMENT

Requirements for OSS may come from various ways discussed below as described by Bart Massey [4]

- Directly the developers
- Users of open-source software
- The implementation of explicit standards
- The emulation of implicit standards
- The need to build learning prototypes

J. Goguen and C. Linde have discussed numerous types of requirements elicitation techniques [3]. Some of them that have been selected for OSSD are mentioned below:

- Questionnaires
- Discussion
- Open ended interviews
- Introspection

These techniques have been selected because they can be easily used for OSS development to elicit the requirements.

A. ANALYSIS OF REQUIREMENTS ELICITATION TECHNIQUES IN OSSD

The above mentioned requirements elicitation techniques have been analyzed for OSS development in this section through the criteria described in the proposed framework.

1. Questionnaires

Questionnaire survey is the most suitable technique for gathering requirements for open source software because the developers can interview the community members and can ask what they need besides the users can also add what they exactly want. The advantage of using this technique is that the questionnaires can be made available to the users through internet or other sources. Along with the advantages, the disadvantage of this technique is that the developer may not get the right choices of users [3]. These types of interviews can be of two type open ended or close ended. Open ended questionnaires allows the user to explain their requirements about the software where as in close ended questionnaires, the user has only the choice of selecting what the developer has thought of.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Questionnaire elicitation technique has been analyzed according to the proposed framework below:

- **Adaptable:** This elicitation method can work best to generate requirements in multiple environments but introspection and discussion has a little edge over this method. In OSS development requirements can be generated through questionnaire till a certain stage.
- **Usable:** This technique can be used to achieve effectiveness, efficiency and satisfaction. Efficiency refers to the resources required to achieve the requirement elicitation goals. Effectiveness refers to level of accuracy and completeness. Satisfaction refers to the user's acceptability of the product. This elicitation method helps to achieve high effectiveness and greater satisfaction with fewer resources for and during OSS development.
- **Implementable:** This method is not overly complex and can be executed very easily by the developers of the product. The developers can distribute the questionnaires over the internet to get quick response.
- **Understandable:** As the requirements gathered using questionnaires elicitation method are described by the intended users of the system so they are not complicated and are simple to understand.
- **Ease of Communication:** Ease of communication in requirement elicitation refers to how easily requirements are indicated. So the requirements are very easily specified using questionnaires during OSS development.
- **Reflects Stakeholders Goal:** It means acceptance of the product's requirements by stakeholder. Stakeholders are likely to agree to the requirements. There is less probability of reflection of stakeholder's goal using this elicitation method for OSS development.
- **Remote Administration:** Remote Administration is difficult to achieve during OSS development through Questionnaire.
- **Time Constraints:** During OSS development questionnaire is a time consuming process for eliciting requirements because it takes a lot of time to gather data and then formulate the data for obtaining useful results.
- **Cost Free:** For OSS Development Questionnaire is not a cost free procedure for requirements elicitation as developing the questionnaire and distributing it by any means and then gathering the information depicted in the questionnaires requires resources.

2. Discussion

Another extensively used technique by the open source developers is discussion with the users. This technique focuses on community discussions and deciding what the community wants and developers present their opinion about what is possible or in what way it could happen [1]. Through discussions, users and developers interact with each other and try to solve the problem that has been raised. Discussions can be among group or with individuals through internet, mail post, telephone or any other source. The advantage of discussions in OSSD is that the both the developers and the users interact with each other to get an idea what is to be developed. The drawback of this technique is that there may arise conflicts among community members. Discussion technique for eliciting OSSD requirements has been analyzed according to the criteria below:

- **Adaptable:** This method can be used to generate requirements in multiple environments. This elicitation methods works well in the products initial planning stages till the products final stage.
- **Usable:** This technique can be used to achieve effectiveness, efficiency and satisfaction. But this technique is not as best as introspection and questionnaire but it is good at its place. Efficiency refers to the resources required to achieve the requirement elicitation goals. Effectiveness refers to level of accuracy and completeness. Satisfaction refers to the user's acceptability of the product. This elicitation method helps to achieve high effectiveness and greater satisfaction with fewer resources for and during OSS development.
- **Ease of Communication:** Ease of communication in requirement elicitation refers to how easily requirements are indicated. So the requirements are very easily indicated using discussion during OSS development.
- **Implementable:** This method is not overly complex and can be executed easily.
- **Understandable:** It is very easy to understand the requirements gathered using discussion elicitation method.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- **Reflects Stakeholders Goal:** It means acceptance by stakeholder. Stakeholders are likely to agree to the requirements. There is a likely probability of reflection of stakeholder's goal using this elicitation method for OSS development.
- **Remote Administration:** During OSS development remote administration can be best achieved with discussion. Through discussion from products initial planning stage to final product stage remote administration can be easily done and can monitor the requirements of the software very well.
- **Time Constraints:** Discussion is also a time consuming process because several things have to be kept in mind while doing discussion and several arrangements have to be made for this purpose. Moreover, discussion is done at each stage of software development so at each stage knowledge of previous stage should be known or clear to the person.
- **Cost Free:** For OSS Development discussion is not a cost free procedure for requirements elicitation because the developers or stakeholders may not be in the same location.

3. Open Ended Interviews

Interviews are the most prior form of gathering requirements in which the developers ask the users about their needs [6].These types of interview provide a great ease to software developers for OSS as the developers can use this elicitation technique to publish open ended interviews on internet and can get the response of the user community as well as new ideas can be generated to improve the requirements already written. Open ended interviews provide the public a chance to express their needs instead of only sticking to the developers ideas [1]. Open ended interviewing technique has been analyzed for OSSD below:

- **Adaptable:** In OSS development this method cannot be used to generate requirements in multiple environments. This elicitation methods works well in the products initial planning stages.
- **Usable:** This technique can be used to achieve effectiveness, efficiency and satisfaction. But this technique is not as best as introspection and questionnaire but it is good at its place. Efficiency refers to the resources required to achieve the requirement elicitation goals. Effectiveness refers to level of accuracy and completeness. Satisfaction refers to the user's acceptability of the product. This elicitation method helps to achieve high effectiveness and greater satisfaction with fewer resources for and during OSS development.
- **Ease of Communication:** Ease of communication in requirement elicitation refers to how easily requirements are indicated. So the requirements are very easily indicated using open-ended interviews during OSS development.
- **Implementable:** This method is not overly complex but can be executed with effort.
- **Understandable:** It is very easy to understand the requirements gathered using open-ended interviews elicitation method.
- **Reflects Stakeholders Goal:** It means acceptance by stakeholder. Stakeholders are likely to agree to the requirements. There is a likely probability of reflection of stakeholder's goal using this elicitation method for OSS development.
- **Remote Administration:** Remote Administration is difficult to achieve during OSS development through open-ended interviews due to time constraints that is when the developer is available the stakeholder may be unavailable, different locations of the interviewer and interviewee.
- **Time Constraints:** Open-Ended Interviews is also a time consuming process because it takes a lot of time to make the idea clear to the user and gather the useful requirements from the user.
- **Cost Free:** For OSS Development Open-Ended Interviews is not a cost free procedure for requirements elicitation.

4. Introspection

Introspection means deriving requirements through thoughts and imaginations. It is an important elicitation technique because it serves as an initiator for other techniques [7]. This technique is also very useful in OSSD because the developer is the only person who derives requirements for the OSS that is to be developed as well as this technique is cost free. But the problem with this technique is that the developer may not have same understanding of the requirements as those of users [1]. Introspection for

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

eliciting requirements of OSSD has been analyzed according to the framework below:

- **Adaptable:** In OSS development this elicitation method works best to generate requirements in multiple environments i.e. it works well when the product is in its completion stage as well as when it is in the planning stage.
- **Usable:** This technique can be best to achieve effectiveness, efficiency and satisfaction. Efficiency refers to the resources required to achieve the requirement elicitation goals. Effectiveness refers to level of accuracy and completeness. Satisfaction refers to the user's acceptability of the product. This elicitation method helps to achieve high effectiveness and greater satisfaction with fewer resources for and during OSS development
- **Ease of Communication:** Ease of communication in requirement elicitation refers to how easily requirements are indicated. So the requirements are not easily indicated using introspection during OSS development. As introspection is done by developer so not all the requirements are indicated by the developer. They may differ from user to developer.
- **Implementable:** This method is not overly complex and can be executed very easily by the developers.
- **Understandable:** This elicitation method is easy to understand but require a little effort in understanding the requirements of the system if the developer is not much familiar with the problem domain.
- **Reflects Stakeholders Goal:** Stakeholders are likely to agree to the requirements proposed by the developer through introspection but there is less probability of reflection of stakeholder's goal using this elicitation method for OSS development as these requirements are elicited independently by the developer.
- **Remote Administration:** During OSS development remote administration can be best achieved through introspection. As all the requirements are elicited by the developer so he can do the remote administration very well because he knows what the requirements of the system are.
- **Time Constraints:** Introspection is not a time consuming process for eliciting requirements during OSS development because this involves imagination by the developer.
- **Cost Free:** For OSS Development Introspection is a cost free procedure for requirements elicitation as the developers are the ones who elicit requirements using their own understanding and acquaintance about the problem domain through imagination or thoughts.

TABLE 2: Comparison of requirements elicitation techniques for OSSD

Technique	Type of Data	Good For	Merits	Demerits
Questionnaires	Qualitative & Quantitative Data	Getting particular response	Can be made available to everyone in less resources	Accurate response may not be received
Discussion	Mostly qualitative, some quantitative data	Gathering various opinions	Depicts the agreements and disagreements among people	No consensus may be reached
Open ended interviews	Some quantitative, mostly qualitative data	Investigating problems	Users can express how and what they need	A large amount of data is gathered
Introspection	Qualitative Data	Initiating other requirements elicitation techniques	Free of cost	Much experience professional required

VII. APPLYING PROPOSED METHODOLOGY TO ELICIT REQUIREMENTS

Mozilla Firefox is an example of open source web browser that is developed for operating systems like Microsoft Windows, Mac OS X and Linux. It is the most secure web browsers available these days [5]. To understand the proposed model, formula and the framework, this section presents a case study of a proposed new add-on for Mozilla Firefox named as a multi-messenger button. The purpose of this add-on is to provide the web browser users to login to their messengers by using this simple button and without installing several different messengers which occupies a lot of storage space. To elicit its requirements, techniques have to be selected by using the criteria framework.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

To elicit the requirements the proposed formula for gathering requirements will be used.

$Et = (C(T_i) \cap Ev(T_i), P) \rightarrow \{Et \in T \mid Et \text{ is applicable to some specific problem}\}$

The problem (P) identified by the developer is that the users have to minimize their web browsers to communicate using the messengers as well as installing different messengers consume a lot of storage space.

RA = Knowledge ⟶ Problem Domain ⟵ Expertise

Criteria has been applied onto the elicitation techniques for selection of appropriate technique(s) and techniques selected after comparison are discussion and introspection that are most suited for this case study. Other techniques have their own merits and demerits and may be suitable for some other OSS project. The comparison of elicitation techniques according to the criteria framework for this product is as follows:

TABLE 3: Criteria Framework applied on techniques for proposed product

Criteria	Techniques			
	Introspection	Discussion	Open Ended Interviews	Questionnaires
Adaptable	+++	+++	-	-
Usable	+++	+++	-	-
Ease of Communication	+++	++	-	-
Understandable	+++	+++	+	+
Implementable	+++	+++	-	-
Reflect Stakeholder's Goals	++	++	+++	+
Remote Administration	+++	+++	+++	+++
Time Constraints	-	++	+++	+++
Cost Free	+++	+	++	+

According to the table above, it can be noted that introspection and discussion are the most appropriate techniques for the development of this product. Introspection and discussion both fulfills most of the criteria for eliciting requirements as both these techniques are adaptable, usable and there are only developers who have thought to implement this idea so ease of communication is also fulfilled. Understandability is a measure of how easily the technique can be understood by the developer so as introspection is based on thoughts and imaginations of the developer so it also fulfills this criterion whereas discussion among developers (if there is more than one person developing the product) is also easy to understand. Both these techniques are implementable, reflects developers thoughts so fulfills accuracy criteria as well as stakeholder's goals. These techniques can be administered remotely and for introspection there are no timing constraints. For discussion timing constraints can occur in such a way that a developer may not be available for discussion. Both these techniques are cost free if the developers are in the same geographic location but discussion may be costly if the developers are dispersed on more than one location.

The techniques have then been evaluated according to the product being developed as this is a small scale project so selection of an elicitation technique which requires minimum resources and end user involvement should be selected.

TABLE 4: Evaluation of techniques according to proposed product

Technique	Effective	Resources Required	End User Involvement
Introspection	Yes	Nil	No
Questionnaires	No	Cost, Time, Set of Questions	Yes
Discussion	Yes	Time	May Be
Open Ended Interviews	No	Cost, Time, Questions for interview	Yes

By applying the criteria onto techniques and then evaluating them according to the proposed product, two techniques introspection and discussion are selected as the most appropriate ones for this type of product. Hence Et = (Introspection, Discussion)

When Et is applied on to the problem to elicit requirements following requirements have been gathered.

$R_i = Et(P_i) \cup RA$ where $R_i = \{R_1, R_2 \ldots R_n\}$

Some of the requirements asserted through introspection based on developer's knowledge and

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

experience for multi-messenger button add-on for Mozilla Firefox are shown in Table 5:

TABLE 5: Requirements Asserted (RA) through Introspection

S. No.	Requirements
R1	All messengers must appear in a single window interface.
R2	The window interface must be tabbed for each messenger.
R3	User must be able to create a new login id for any messenger.
R4	Messenger must authenticate each user.
R5	All messenger settings must be separated from each other.
R6	There should be no intermixing of contacts.
R7	Messenger must have a simple and user friendly interface.

Requirements gathered through discussions are shown in Table 6.

TABLE 6: Requirements gathered through Discussion

S. No.	Requirements
R1	There must be an option to logout from all messengers using a single click.
R2	The user should be able to create a single login ID to access all accounts.
R3	The window for messenger must remain open while working on browser.
R4	The user must be notified when an IM is received even if the browser is minimized.
R5	The user must be able to change the settings.

The union of both these requirements is the set of final requirements that have been elicited for the proposed add-on for Mozilla Firefox. OSS provides its users with the ease to update or modify the software after development. If end users are not satisfied with the developed product the source code for the software is freely available to them so that they can continue adding requirements and modify the product according to their own needs and expectations.

VIII. CONCLUSION & FUTURE WORK

Requirements elicitation is the most vital and complicated phase of the software development. For OSSD the most part of this phase is done by the developer with a little involvement from the user community. In this paper, we have discussed requirements elicitation process for open source software development. We have proposed a model for the requirements elicitation process and proposed a formula for eliciting the requirements of open source software development. Some of the requirements elicitation techniques suited for OSSD have been selected. Also a criteria framework for the comparison of techniques according to the OSSD has been developed which focuses on the selection of elicitation techniques for open source software development. This framework has been explained in detail with the help of a proposed OSS product and requirements are elicited. We have also compared these techniques and discussed their merits and demerits.

In this paper, we have covered some of the elicitation techniques for open source software development. In future, other techniques will be evaluated and analyzed according to the proposed framework and requirements elicitation model. Although there are many techniques for requirements elicitation of OSS development but each of the technique has its own merits and demerits and if one technique is good for one project it may not be for the other.

REFERENCES

[1] Henderson, “Requirements Elicitation in Open-Source Programs”, CrossTalk The Journal of Defense Software Engineering 2000, Volume: 13, Issue: 7

[2] Scacchi, “Understanding Requirements for Developing Open Source Software Systems”, Software IEEE Proceedings, Volume 149, Issue 1, Journals & Magazines, 2002

[3] J.A. Goguen, C. Linde: “Techniques for Requirement Elicitation”, Proceedings of IEEE International Symposium on Requirements Engineering, 1993

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[4] Bart Massey, "Where Do Open Source Requirements Come From (And What Should We Do About It)", A Position Paper for the Second ICSE Workshop on Open Source Software Engineering, 2001

[5] John Noll, "Innovation in Open Source Software Development", IFIP International Federation for Information Processing, 2007, Volume 234, Open source Development, Adoption and Innovation, pages 109-120

[6] Foddy W, "Constructing questions for interviews and questionnaires", Cambridge University Press, Cambridge, Edition 1, 1994

[7] Shams-Ul-Arif, Qadeem Khan, Gahyyur: "Requirements Engineering Processes, Tools/Technologies, & Methodologies", International Journal of Reviews in Computing, 2010

[8] Audris Mockus, Roy T. Fielding und James Herbsleb, "A Case Study of Open Source Software Development: The Apache Server" ACM , 2000

[9] Dengya Zhu, Vidyasagar Potdar, and Elizabeth Chang, "Open Source Software Development (OSSD) Based On Software Engineering", Springer, Conference Paper, 2006.

[10] Crowston, Scozzi, "Exploring the Strengths and Limits of Open Source Software Engineering Processes: A Research Agenda", Journal Article: Former Departments, Centers, Institutes and Projects, 2002

[11] Eric S. Raymond, "The Cathedral and the Bazaar: Musingson Linux and Open Source by an Accidental Revolutionary", O'Reilly & Associates, 1999

[12] Vinay Tiwari, "Software Engineering Issues in Development Models of Open Source Software", IJCST Vol. 2, Issue 2, June 2011

[13] Fox C, "Introduction to Software Engineering Design, Processes, Principles, and Patterns with UML 2", Boston, Massachusetts: Pearson/Addison Wesley, 2007

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Log Analysis Techniques using Clustering in Network Forensics

Imam Riadi[1]
[1]Department of Information System, Faculty of Mathematics and Natural Science,
Ahmad Dahlan University,
Yogyakarta,Indonesia
imam_riadi@uad.ac.id

Jazi Eko Istiyanto[2], Ahmad Ashari[2], Subanar[3]
[2]Department of Computer Science and Electronics,
[3]Department of Mathematics,
[2,3]Faculty of Mathematics and Natural Sciences,
Gadjah Mada University, Yogyakarta, Indonesia
{jazi,ashari}@ugm.ac.id, subanar@yahoo.com

Abstract — Internet crimes are now increasing. In a row with many crimes using information technology, in particular those using Internet, some crimes are often carried out in the form of attacks that occur within a particular agency or institution. To be able to find and identify the types of attacks, requires a long process that requires time, human resources and utilization of information technology to solve these problems. The process of identifying attacks that happened also needs the support of both hardware and software as well. The attack happened in the Internet network can generally be stored in a log file that has a specific data format. Clustering technique is one of methods that can be used to facilitate the identification process. Having grouped the data log file using K-means clustering technique, then the data is grouped into three categories of attack, and will be continued with the forensic process that can later be known to the source and target of attacks that exist in the network. It is concluded that the framework proposed can help the investigator in the trial process.

Keywords : analysis, network, forensic, clustering, attack

I. INTRODUCTION

Together with the rapidity of internet network development, there are countless individual and business transactions conducted electronically. Communities use the Internet for many purposes including communication, email, transfer and sharing file, search for information as well as online gaming. Internet network offers users to access information that is made up of various organizations. Internet development can be developed to perform digital crimes through communication channels that can not be predicted in advance. However, development of the Internet also provides many sources of digital crime scene. Internet crime is now increasing [1], for example, employees accessing websites that promote pornography or illegal activities that pose a problem for some organizations. Pornography has become a huge business and caused many problems for many organizations. Not only easily available on the Internet but perpetrators also frequently spreading pornography using the advances of Internet technology to attack computer with unsolicited email and pop up ads that are not desirable. Some form of pornography is not only illegal but also bring a big problem for digital investigators. However posting child pornography on the Internet can help lead investigators to the victim. As well as threatening letters, fraud, intellectual property theft is a crime that leaves a digital footprint [2].

Cyber crime, a crime using information technology as instrument or target, have led to the birth of network forensic in response to the rise of the case. Improving the quality of tools and techniques for network forensic analysis is needed to deal with cyber criminals that are more and more sophisticated. Digital forensics, in essence, answer the question: when, what, who, where, how and why related to digital crime [3]. In conducting an investigation into the computer system as an example: when referring to the activity observed to occur, what activities related to what is done, who related to the person in charge, where related to where the evidence is found, how related to activities conducted and why, the activities related to why the crime was committed. Legal regulation of criminal act in the field of information technology is arranged in Law No 11 of 2008 that contains about information and electronic technologies (ITE) contained the provisions of the criminal act elements or the acts that are prohibited in the field of ITE, such as in Article 27, 28, 29, 30, 31, 32, 33, 34, 35 and Article 36. Currently, Indonesian government and House of Representatives are processing on the Information Technology Crime Bill that is included in 247 list of Prolegnas Bill, 2010-2014 [4].

Consequence with many crimes using information technology particularly using the Internet, some crimes are often carried out in the form of attacks that occur within a particular agency or institution. To find and identify the types of attacks, requires a long process that requires time, human resources and utilization of information technology to solve these problems. The process of identifying attacks that happened also needs the support of both hardware and software as well. The attack happened in the Internet network can generally be stored in a log file that has a specific data format. To simplify the process of analyzing the log, the use of scientific methods to help a diverse group of raw data is needed. Clustering technique is one of methods that can be used to help facilitate the identification process.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

II. CURRENT STUDIES ON NETWORK FORENSICS

A. Forensics in Computer Security

The rapidity of information technology development especially in the field of computer network has brought a positive impact that make human activity becomes easier, faster and cheaper. However, behind all the conveniences it was the development of such infrastructure services have a negative impact emerging in cyberspace, among others: the theft of data on the site, information theft, financial fraud to the Internet, carding, hacking, cracking, phishing, viruses, cybersquating and cyberporn. Some crimes, especially that are using of information technology services spesifically the Internet network can be used to perform some illegal activities that harm others, such as: cyber gambling, cyber terrorism, cyber fraud, cyber porn, cyber smuggling, cyber narcotism, cyber attacks on critical infrastructure, cyber blackmail, cyber threatening, cyber aspersion, phishing.

The number of computer crime cases and computer related crime that is handled by Central Forensic Laboratory of Police Headquarters at around 50 cases, the total number of electronic evidence in about 150 units over a period of time as it can be shown in Table 1. [5].

Table 1. The number of computer crimes and computer related crime cases

year	number of cases
2006	3 cases
2007	3 cases
2008	7 cases
2009	15 cases
2010 (May)	27 cases

The forensic process began has been introduced since long time. Several studies related to the forensic process include [5]:

a) Francis Galton (1822-1911); conducted the research on fingerprints
b) Leone Lattes (1887-1954); conducted the research on blood groups (A, B, AB & O)
c) Calvin Goddard (1891-1955); conducted the research on guns and bullets (Ballistic)
d) Albert Osborn (1858-1946); conducted the research on document examination
e) Hans Gross (1847-1915); conducted scientific research on the application of the criminal investigation
f) FBI (1932); conducted the research using Forensic Lab

The forensic process requires a few tools that can help perform forensic processes, Some computer forensic software are shown in Table 2.

Table 2. Forensic Computer Tools

No	Software	Information
1	E-Detective	http://www.edecision4u.com/
2	Burst	http://www.burstmedia.com/release/advertisers/geo_faq.htm
3	Chkrootkit	http://www.chkrootkit.org
4	Cryptcat	http://farm9.org/Cryptcat/
5	Enterasys Dragon	http://www.enterasys.com/products/advanced-security-apps/index.aspx
6	MaxMind	http://www.maxmind.com
7	netcat	http://netcat.sourceforge.net/
8	NetDetector	http://www.niksun.com/product.php?id=4
9	NetIntercept	http://www.sandstorm.net/products/netintercept
10	NetVCR	http://www.niksun.com/product.php?id=3
11	NIKSUN Function Appliance	http://www.niksun.com/product.php?id=11
12	NetOmni	http://www.niksun.com/product.php?id=1
13	Network Miner	http://sourceforge.net/projects/networkminer/
14	rkhunter	http://rkhunter.sourceforge.net/
15	Ngrep	http://ngrep.sourceforge.net/
16	nslookup	http://en.wikipedia.org/wiki/Nslookup
17	Sguil	http://sguil.sourceforge.net/
18	Snort	http://www.snort.org/
19	ssldump	http://ssldump.sourceforge.net/
20	tcpdump	http://www.tcpdump.org
21	tcpxtract	http://tcpxtract.sourceforge.net/
22	tcpflow	http://www.circlemud.org/~jelson/software/tcpflow/
23	truewitness	http://www.nature-soft.com/forensic.html
24	OmniPeek	http://www.wildpackets.com/solutions/network_forensics
25	Whois	http://www.arin.net/registration/agreements/bulkwhois
26	Wireshark	http://www.wireshark.org/
27	Kismet	http://www.kismetwireless.net/
28	Xplico	http://www.xplico.org/

CERT defines the forensic as the process of collecting, analyzing, and presenting evidence scientifically in court. Computer forensics is a science to analyze and present data that have been processed electronically and stored in computer media [1]. Digital forensics is the use of scientific methods of preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources or proceeding to facilitate the reconstruction of the crime scene [6].

Indonesia has a state law that can be used to help confirm that crime committed using information technology services may be subject to Article 5 of Law no. 11/2008 on Information and Electronic Transactions (UU ITE) states that electronic information and or electronic documents and or prints with a valid legal evidence can be used as guidelines for processing the crime to the courts, the mechanism of digital evidence uses as adapted to the rules of evidence contained in the investigation.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

A few incidents of crimes that often occur in the computer [2]. Digital evidence is defined as the evidentiary value of information stored or transmitted in digital form [7]. A potential source of digital evidence has been growing in the field of mobile equipment [8], Gaming console [9], and digital media devices [10]. Other unique properties of digital evidence is that it can be duplicated. As a result, the evidence must be stored properly at the time of the analysis performed on the copy or copies to ensure that the original evidence was accepted in court [11].

B. Internet Forensics

American law enforcement agencies began working together in addressing the growing of digital crime in late 1980 and early 1990. Rapid growth of Internet technologies along with increasing volume and complexity of digital crime makes the need for network forensics Internet becomes more important. A state which is not expected to change the future given the number of incidents increased steadily. Figure 1. claimed an increasing number of incidents reported by CERT. [1]

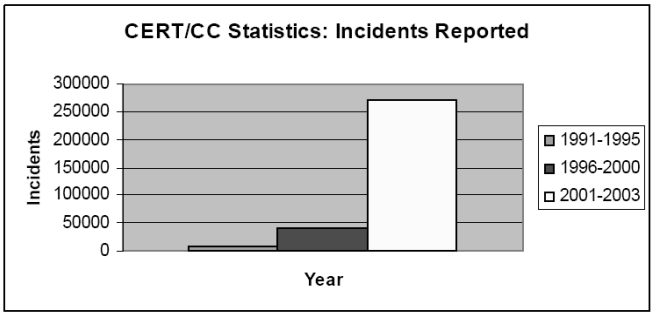


Figure 1. Report the number of incidents by the CERT

C. Network Forencics

Network forensics is an attempt to prevent attacks on the system and to seek potential evidence after an attack or incident. These attacks include probing, DoS, user to root (U2R) and remote to local.

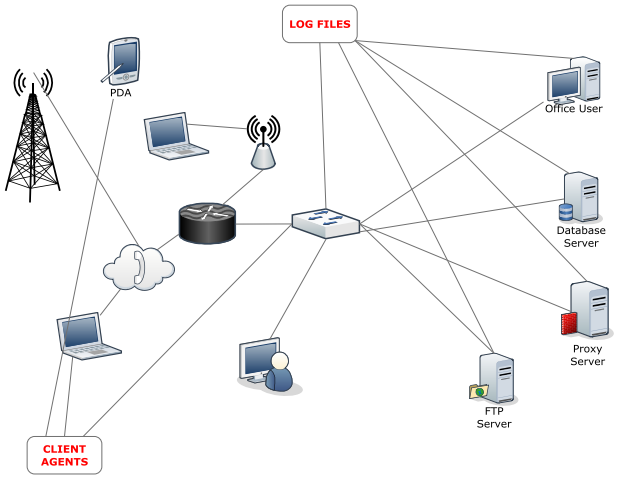


Figure 2. Picture of network forensics process

Figure 2 provides an overview of a network forensics process that occurs within an organization [12]. Network forensics is the process of capturing, recording and analyzing network activity to find digital evidence of an assault or crimes committed against, or run using a computer network so that offenders can be prosecuted according to law [12]. Digital evidence can be identified from a recognizable pattern of attack, deviation from normal behavior or deviations from the network security policy that is applied to the network. Forensic Network has a variety of activities and techniques of analysis as an example: the analysis of existing processes on IDS [13], analysis of network traffic [14] and analysis of the network device itself [15], all of them are considered as the part of network forensics.

Digital evidence can be gathered from various sources depend on the needs and changes in the investigation. Digital evidence can be collected at the server level, proxy level or some other source. For example the server level digital evidence can be gathered from web server logs that store browsing behavior activities that are frequented. The log describes the user who access the website and what are they do. Several sources including the contents of network devices and traffic through both wired and wireless networks. For example, digital evidence can be gathered from the data extracted by the packet sniffer like: tcpdump to monitor traffic entering the network [16].

III. THEORETICAL BACKGROUND

A. Network Abnormal Detection in Computer Security

Anomaly detection refers to the problem of finding patterns in data that are inconsistent with expected behavior. Patterns that do not fit often called as an abnormal condition that often occurs within a network. The detection of abnormal tissue can be found in several applications such as credit card fraud detection, insurance or health care, intruder detection for network security, fault detection is critical to the system as well as observations on the military to find enemy activity. Anomaly detection can translate the data in significant so way that it can present information that is useful in various application domains. For example, the presence of abnormal patterns that occur in network traffic that can be interpreted that the hacker sends sensitive data for unauthorized purposes [17].

B. The concept of Network Abnormal Detection

Anomaly patterns in the data that do not fit well with the notion of normal behavior. Figure 3 depicts anomalies in a simple 2-dimensional data that have been defined, which has two normal regions, N1 and N2, because the most frequent observation in a two-way areas [17]. Examples of points O1 and O2, and O3 point in the region, are the anomalies.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

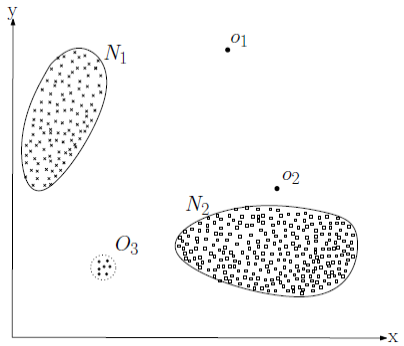


Figure 3. a simple example of an anomaly in the data 2-dimensional.

Anomaly may be caused by many things, for example malicious activities, like credit card fraud, terrorist activities or making hang the system, but all reason have common characteristics that it is interesting to be analyzed. Above caused most of the abnormal is not easy to solve. Most of the abnormal detection techniques can solve these problems. Detection of abnormal has become a major topic in research, [18] among others provides a broad survey of the abnormal detection techniques are developed using machine learning and statistical domains. Review techniques for detection of abnormal numerical data by [19]. Review of detection techniques using neural networks and statistical approaches by [20] and [21].

C. Clustering

Clustering is a process to make the grouping so that all members of each partition has a certain matrix equation based on [22]. A cluster is a set of objects that were merged into one based on equality or proximity. Clustering as a very important technique that can perform translational intuitive measure of equality into a quantitative measure. Here is an example of the clustering process as shown in Figure 4 [22].

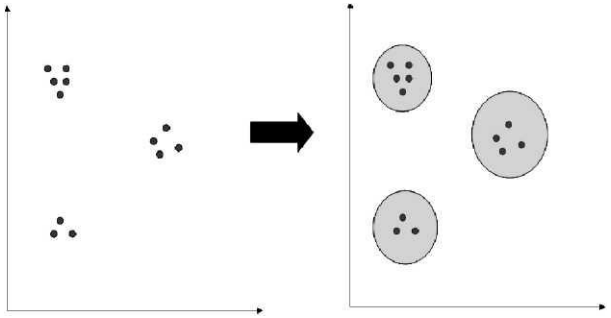


Figure 4. Clustering based on proximity

Figure 4. is an example of the process of clustering the data using proximity as a parameter. The data that are near will be clustered each other as a member of the cluster. Clustering characteristics can be grouped into 4 types as described below :

a) Partitioning clustering
Partitioning clustering is also called exclusive clustering, where each data must belong to a particular cluster. Characteristics of this type also allow for any data that includes a specific cluster in a process step, the next step moving to another cluster.
Example: K-Means, residual analysis.

b) Hierarchical clustering
In the hierarchical clustering, every data must belong to a particular cluster, and the data that belongs to a particular cluster at a stage of the process can not move to another cluster at a later stage.
Example: Single Linkage, Centroid Linkage, Complete Linkage, Average Linkage.

c) Overlapping clustering
In overlapping clustering, each data allows belong to multiple clusters. The data has a value of membership (membership) in a cluster.
Example: Fuzzy C-means clustering, Gaussian Mixture.

d) Hybrid
Hybrid characteristics is the cluster characteristics that combines the characteristics of the clustering characteristics of the partitioning, overlapping, and hierarchical

Grouping method is basically divided into two, namely the method of grouping hierarchy (Hirarchical Clustering Method) and the method of Non Hierarchy (Non Hirarchical Clustering Method). Hierarchical clustering method is used when no information on the number of groups to be selected. While the non-hierarchical clustering method aims to classify objects into k groups (k <n), where the value of k has been determined previously. One of the Non Hierarchical clustering procedure is to use K-Means method. This method is a method of grouping which aims to group objects so that the distance of each object to the center of the group within a group is the minimum [22].

D. K-Means Clustering

K-means is included in the partitioning clustering that also called exclusive clustering separates the data into k separate parts and each of the data should belong to a particular cluster and allows for any data that includes a specific cluster in a process step, the move to the next stage cluster other [22]. K-means is algorithm that is very famous because of its ease and ability to perform the grouping of the data and outliers of data very quickly. In the K-means any data should be included into a specific cluster, but allows for any data that includes a specific cluster in a process step, the next step moving to another cluster. Figure 5 shows illustration of the process steps clustering using K-means algorithm [22] as follows :

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

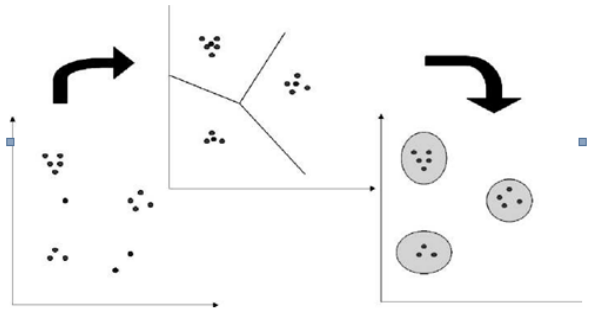


Figure 5. Illustration of the process steps clustering using K-means algorithm.

K-Means algorithm on clustering can be done by following these steps [22]:

a) Determine the number of clusters k to be formed.
b) Generate k centroids (cluster center) beginning at random.
c) Calculate the distance of each data to each centroid.
d) Each data choose the nearest centroid.
e) Determine new centroid position by calculating the average value of the data that choose the same centroid.
f) Return to step 3 if the new centroid position is not same with the old centroid.

Here are the advantages of K-means algorithm in the clustering process [22]:

a) K-means is very fast in the clustering process.
b) K-means is very sensitive to the random generation of initial centroid.
c) Allows a cluster has no members
d) The results of clustering with K-means is not unique (always changing), sometimes good, sometimes bad
e) K-means is very difficult to reach the global optimum

Moreover, K-means algorithm has a drawback that the clustering results are very dependent on the initialization initial centroids that are randomly generated, and therefore allows for any particular cluster of data that includes a process step, the next stage move to another cluster. In the net stage Figure 6 illustrates the weakness of K-means algorithm showed that in the previous stages there are three clusters with a cluster which do not have any member and on the next stage there is cluster formation that is just consist of two cluster and all of them have members [22], of course this is caused by the centroid that is operated at random.

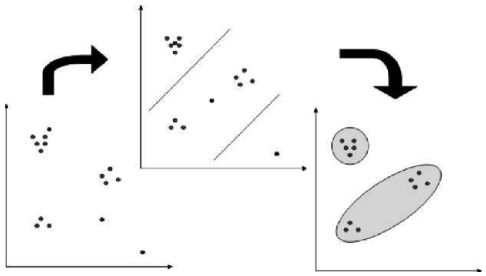


Figure 6. Illustration of K-means algorithm weakness.

IV. CASE STUDY

Topology that used in this research aims to facilitate the investigation process is shown in Figure 7.

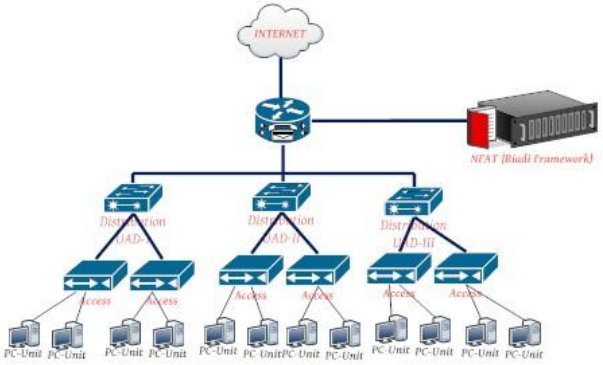


Figure 7. The design of topology research

Framework Module NFAT (Network Forensic Analysis Tool) is developed using open source software that can run on any operating system platform, among others (Linux, Unix, FreeBSD, OpenBSD), this application was developed with shell scripting, combined with PHP and supported using the MySQL DBMS.
Experiments and testing framework NFAT module is done at the Center for Computer Laboratory Ahmad Dahlan University, Yogyakarta, to obtain the appropriate data for the data traffic flowing in a computer network is large enough.

This research will be developed using a framework that is shown in Figure 8

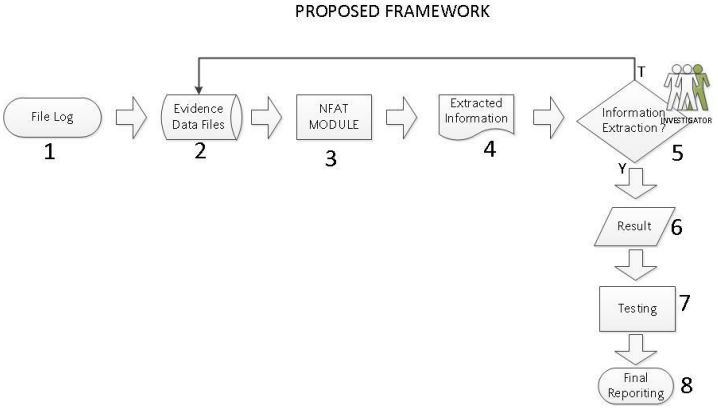


Figure 8. Model Framework to be developed

In Figure 8. First-stage of forensic process starting from the collection of evidence collected in connection with the initial written by the investigators as evidence profiles and the input to the database of evidence, evidence management system sought by finding the appropriate case-related data and time. In the analysis phase, the input data generated by the log file system, then the database will be stored in evidence. When the investigator and the investigator needs information, the information extracted from Module NFAT (Network Forensic Analysis Tools). At the investigation stage, the extracted information is considered as part of the investigation.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Although it is very fast final decision depends on the investigator. Investigator will determine whether the evidence has been produced to meet or not, if the evidence has not been met, it will be back again to extract data from evidence database. Otherwise if the evidence meets the test process will be done to verify that the data is original and suitable with the criteria of evidence that required by investigators. In the final stage of reporting, digital evidence will be presented in a particular format so that it can help the investigator in the trial process.



Figure 9. Framework Module NFAT

NFAT module as shown in Figure 9 works using K-means clustering algorithm which can perform the detection of attacks based on grouping the data into three groups of attacks, namely [22]:

a) dangerous attack,
b) rather dangerous attack,
c) not dangerous attack.

Based on the data stored in the database log file system, then the clustering process will be done in stages as follows [22]:

a) Specified value of k as the number of clusters to be formed.
b) Generate k centroids (cluster center) beginning at random.
c) Calculate the distance of each data to each centroid.
d) Each data choose the nearest centroid.
e) Determine new centroid position by calculating the average value of the data that choose the same centroid.
f) Return to step c if the new centroid position is not same with the old centroid.

The results of the data cluster for an attack is highly dependent on the generation of its centroid because it is done at random, this resulted in the detection of an attack on the data is always changing. Once the data clustering process is carried out the attack, then each cluster results do cluster labeling is included in the hazard, rather dangerous or not dangerous. Then from the cluster that has been labeled, checked against is done against the data which are entered into the next group of malicious attacks on the note in the report. The process of clustering using K-means algorithm is shown in Figure 10 [22].

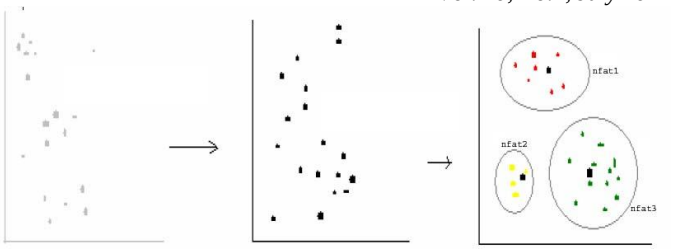


Figure 10. The process of clustering the data with the K-means attack

From the data mentioned above cluster that are formed is the best cluster obtained from the cluster that has the smallest variance. Of the above forms clusters, each cluster for the data had been formed but has not been labeled, the labeling is done by calculate for the matrix multiplication of the final centroid of each cluster is multiplied by its transpose matrix so we get a scalar value of each cluster, as shown in Table 3 [22].

Table 3. Cluster grouping type of attack

No	Cluster	ID
1	nfat1	1,3,6,7,10,16
2	nfat2	9,11,12,13
3	nfat3	2,4,8,14,15,17

From the result of transpose multiplication each centroid of three cluster above for example the results obtained with the sequence results from the largest to the small cluster nfat1, nfat2 and cluster nfat3 cluster, The cluster having the highest transpose multiplication result would be labeled as the dangerous cluster. So that the matrix multiplication of the cluster was obtained by labeling the cluster nfatl is a malicious attack, an attack cluster is somewhat harmful nfat2 and nfat3 is not dangerous cluster attack [22].

In addition it has done in module development framework NFAT (Network Forensic Analysis Tool) to facilitate the forensic process is carried out in accordance with the Internet network research plan that has been made. Here are some of the infrastructure supporting the development of NFAT module framework to facilitate the process of forensic analysis of Internet network. The following log data extracted from the database used to identify the attack as shown in Figure 11.

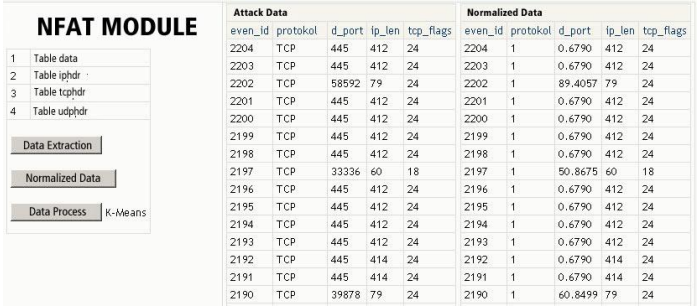


Figure 11. The data used to perform classification of attacks

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The module output data of NFAT is a clustering process, where the results of this cluster can be calculated error values to be compared with the target data that is the target of the cluster. The target data used for comparison are shown in Table 4 [22].

Tabel 4. List of criteria attack

Protocol	Criteria	Port	TCPFlag
TCP	dangerous attack	80,8080,443 20,21 22,23	16,32
	Rather dangerous attack	161,143,162, 110,993	The combination of binary digits 20-24
	not dangerous attack	In addition to the above mentioned	The combination of binary digits 20-27
UDP	dangerous attack	53	-
	Rather dangerous attack	137,161,	-
	not dangerous attack	In addition to the above mentioned	-

Having grouped the data log file using K-means clustering technique, then the data is grouped into 3 categories of attack, and then will resume the forensic process that can later be known to the source and target of the attack on the network, this type of attack which occurs on TCP (Transmission Control Protocol) is shown in Figure 12.

Time	Source Address	Dest. Address	Protocol
2011-04-04 00:10:22	**117.206.82.219**:48836	**203.190.115.150**:445	TCP
2011-04-03 23:14:03	**111.242.1.228**:36316	**203.190.115.150**:445	TCP
2011-04-03 22:55:48	**175.111.91.162**:36647	**203.190.115.150**:80	TCP
2011-04-03 22:27:57	**175.111.91.162**:49792	**203.190.115.150**:80	TCP
2011-04-03 22:27:57	**175.111.91.162**:49793	**203.190.115.150**:80	TCP
2011-04-03 22:27:57	**175.111.91.162**:49793	**203.190.115.150**:80	TCP
2011-04-03 22:27:57	**175.111.91.162**:49794	**203.190.115.150**:80	TCP
2011-04-03 22:27:57	**175.111.91.162**:49794	**203.190.115.150**:80	TCP
2011-04-03 22:27:57	**175.111.91.162**:49792	**203.190.115.150**:80	TCP
2011-04-03 22:27:56	**175.111.91.162**:49792	**203.190.115.150**:80	TCP
2011-04-03 22:27:56	**175.111.91.162**:49792	**203.190.115.150**:80	TCP
2011-04-03 22:14:01	**203.190.115.150**:22	**223.255.224.14**:53480	TCP
2011-04-03 20:44:28	**223.255.224.14**:46991	**203.190.115.150**:3306	TCP
2011-04-03 20:33:43	**10.10.98.75**:1319	**203.190.115.150**:139	TCP
2011-04-03 20:24:34	**223.255.224.14**:53440	**203.190.115.150**:22	TCP
2011-04-03 20:03:42	**180.178.92.56**:62743	**203.190.115.150**:22	TCP
2011-04-03 20:03:01	**180.178.92.56**:62743	**203.190.115.150**:22	TCP
2011-04-03 20:00:30	**118.97.8.17**:61524	**203.190.115.150**:3306	TCP
2011-04-03 20:00:30	**118.97.8.17**:59742	**203.190.115.150**:3306	TCP
2011-04-03 19:18:42	**202.152.202.210**:11891	**203.190.115.150**:3306	TCP
2011-04-03 19:18:33	**202.152.202.210**:11891	**203.190.115.150**:3306	TCP
2011-04-03 18:35:56	**202.152.202.166**:52882	**203.190.115.150**:3306	TCP
2011-04-03 18:35:54	**202.152.202.166**:52780	**203.190.115.150**:3306	TCP
2011-04-03 18:30:29	**203.81.224.227**:8092	**203.190.115.150**:445	TCP
2011-04-03 18:12:48	**118.97.8.17**:57693	**203.190.115.150**:22	TCP
2011-04-03 18:12:46	**203.190.115.150**:22	**118.97.8.17**:57693	TCP
2011-04-03 18:11:45	**118.97.8.17**:57693	**203.190.115.150**:22	TCP
2011-04-03 18:11:43	**203.190.115.150**:22	**118.97.8.17**:57693	TCP

Figure 12. The data that perform the types of attacks occurred on the TCP protocol.

The type of attack that occurred in the UDP (User Datagram protocol) can be shown in figure 13.

Time	Source Address	Dest. Address	Protocol
2011-04-03 03:35:02	**203.190.115.150**:34648	**203.190.112.1**:53	UDP
2011-04-03 03:27:01	**203.190.115.150**:45783	**203.190.112.1**:53	UDP
2011-04-03 03:14:47	**203.190.115.150**:49797	**203.190.112.1**:53	UDP
2011-04-03 03:01:36	**203.190.115.150**:46583	**203.190.112.1**:53	UDP
2011-04-02 12:09:41	**203.190.115.150**:35854	**203.190.112.1**:53	UDP
2011-04-02 12:07:40	**203.190.115.150**:32972	**203.190.112.1**:53	UDP
2011-04-02 09:31:05	**203.190.115.150**:56778	**203.190.112.1**:53	UDP
2011-04-01 10:19:23	**203.190.115.150**:50135	**203.190.112.1**:53	UDP
2011-04-01 10:05:38	**203.190.115.150**:36160	**203.190.112.1**:53	UDP
2011-04-01 09:53:33	**203.190.115.150**:45237	**203.190.112.1**:53	UDP
2011-04-01 09:52:33	**203.190.115.150**:58436	**203.190.112.1**:53	UDP
2011-04-01 09:39:30	**203.190.115.150**:45019	**203.190.112.1**:53	UDP
2011-04-01 09:03:33	**203.190.115.150**:45833	**203.190.112.1**:53	UDP
2011-04-01 08:52:13	**203.190.115.150**:59195	**203.190.112.1**:53	UDP
2011-04-01 08:47:30	**203.190.115.150**:57807	**203.190.112.1**:53	UDP
2011-03-28 18:43:09	**203.190.115.150**:59344	**203.190.112.1**:53	UDP
2011-03-28 18:33:48	**203.190.115.150**:56904	**203.190.112.1**:53	UDP

Figure 13. The data that perform the types of attacks occurred on the UDP protocol.

V. CONCLUSIONS

The first stage of the forensic process starting from collection of evidence which is collected in connection with the initial case that is written by the investigators as evidence profiles and entries to the evidence database, evidence management system is sought by finding the appropriate case related data and time. In the analysis phase, the input data generated by the log file system, then the data will be stored in evidence database. When the investigators need information, the information extracted from Module NFAT (Network Forensic Analysis Tools). At the investigation stage, the extracted information is considered as the part of the investigation. Although that process is very fast, the final decision depends on the investigator. Then the investigator will determine whether the evidence that is produced has been met or not, if the evidence has not been met, it will back again to the extract data from evidence database, otherwise if the evidence has been met, the test process will be done to verify that the data is original and appropriate with the criteria of evidence that is needed by investigator. In the final stage of reporting, digital evidence will be presented in a particular format so that it can help the investigator in the trial process.

ACKNOWLEDGMENT

The authors would like to thank Ahmad Dahlan University (http://www.uad.ac.id) that provides funding for the research, and the Department of Computer Science and Electronics Gadjah Mada University (http://mkom.ugm.ac.id) that provides technical support for the research.

REFERENCES

[1] CERT, CERT/CC Statistics 1988-2005, CERT-Research-Annual-Report. (http: //www .cert. org/stats), 2008

[2] Kruse II, W.G. and Heiser, J.G. Computer forensics: incident response essentials. Addison-Wesley, 2002

[3] Beebe, N.L. and Clark, J.G. A hierarchical, objectives-based framework for the digital investigations process. Proceedings of the fourth Digital Forensic Research Workshop. 2004

[4] Syamsuddin A, Tindak Pidana Khusus, Sinar Grafika, Jakarta, 2011

[5] Alamsyah R, Digital Forensic, Security Day 2010, Inixindo, Yogyakarta, 2010.

[6] SWGDE, Best Practices for Computer Forensics, Scientific Working Group on Digital Evidence, 2007.

[7] Pollitt, M.M. Report on digital evidence. Proceedings of the Thirteenth International Forensic Science Symposium, 2001

[8] Mellars, B. Forensic examination of mobile phones. Digital Investigation, vol. 1, no. 4, pp. 266-272, 2004

[9] Vaughan, C. Xbox security issues and forensic recovery methodology (utilising Linux). Digital Investigation, vol. 1, no. 3, pp. 165-172. 2004

[10] Marsico, C.V. and Rogers, M.K. iPod forensics. International Journal of Digital Evidence, vol. 4, no. 2. 2005

[11] Meyers, M. and Rogers, M. Computer forensics: the need for standardization and certification. International Journal of Digital Evidence, vol. 3, no. 2. 2004

[12] Mukkamala, S. and Sung, A.H. Identifying significant features for network forensic analysis using artificial techniques. International Journal of Digital Evidence, vol. 1, no. 4. 2003

[13] Sommer, P. Intrusion detection systems as evidence. Computer Networks, vol. 31, no. 23-24, pp. 2477-2487. 1999

[14] Casey, E. Handbook of computer crime investigation: forensic tools and technology. Academic Press. 2004

[15] Petersen, J.P. Forensic examination of log files. MSc thesis, Informatics and Mathematical Modelling, Technical University of Denmark, Denmark. 2005

[16] Jacobson, TCPDump-dump traffic on a network. Retrieved February, 2006

[17] Chandola.V, Banerjee.A, Kumar.V, Anomaly Detection : A Survey, A modifed version of this technical report will appear in ACM Computing Surveys, 2009

[18] Hodge, V. and Austin, J. A survey of outlier detection methodologies. Artificial Intelligence Review 22, 2, 85-126. 2004

[19] Agyemang M, Barker K, Alhaj R, A comprehensive survey of numeric and symbolic outlier mining techniques. Intelligent Data Analysis 10, 6, 521 538, 2006

[20] Markou, M. and Singh, S. Novelty detection: a review-part 1: statistical approaches.Signal Processing 83, 12, 2481 2497. 2003a

[21] Markou, M. and Singh, S. Novelty detection: a review-part 2: neural network based approaches. Signal Processing 83, 12, 2499 2521. 2003b

[22] Fauziah L, Computer Network Attack Detection Based on Snort IDS with K-means Clustering Algorithm, ITS Library, 2009

AUTHORS PROFILE



Imam Riadi is a lecturer of the Bachelor Information System Program, Matematics and Natural Science Faculty of Ahmad Dahlan University Yogyakarta, Indonesia. He was graduated as S.Pd. in Yogyakarta State University, Indonesia. He got his M.Kom. in Gadjah Mada University, Indonesia. He is currently taking his Doctoral Program at the Computer Science and Electronics Department of Gadjah Mada University Yogyakarta, Indonesia.



Jazi Eko Istiyanto is a Professor and the Head of Computer Science and Electronics Department, Universitas Gadjah Mada Yogyakarta, Indonesia. He holds a B.Sc in Physics from Gadjah Mada University, Indonesia. He got his Postgraduate Diploma (Computer Programming and Microprocessor), M.Sc (Computer Science) and PhD (Electronic System Engineering) from University of Essex, UK.



Ahmad Ashari is an Associate Professor at Computer Science and Electronics Department of Gadjah Mada University Yogyakarta, Indonesia. He was graduated as Bachelor of Physics in Gadjah Mada University, Indonesia. He received his M.Kom. in Computer Science in University of Indonesia, and received his Dr. techn. in Informatics at Vienna University of Technology, Austria.



Subanar is a Professor at the Department of Mathematics, Gadjah Mada University in Yogyakarta, Indonesia. He was graduated as Bachelor of Mathematics from Gadjah Mada University and Ph.D (Statistics) at Wisconsin University, USA.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

A Comparative Study between Using OWL Technology and Jess Rule Based For Applying Knowledge to Agent Based System

Najla Badie Aldabagh
Computer Sciences Department, Mosul University
Mosul, Iraq
najladabagh@yahoo.com

Ban Sharief Mustafa
Computer Sciences Department, Mosul University
Mosul, Iraq
ahmad_nf2003@yahoo.com

Abstract—the Semantic Web is an extended to the current web where web resources can be manipulated and processed intelligently. User query is semantically analyzed and respond to in intelligent way. A set of technologies are developed to serve this requirement, including Resource Description Framework (RDF), Schema RDF and Web Ontology Language(OWL).

Java Agent Development Framework (JADE) is a software framework to make easy the development of multi agent applications in compliance with The Foundation for Intelligent Physical Agents (FIPA) specifications. Several approaches for building knowledge model for JADE agent can be found. The most promising approach is using OWL ontology based knowledge representation which is one of the main standards for the Semantic Web proposed by World Wide Web Consortium (W3C), and it is based on description logic. Representing knowledge based on ontology provides many benefits over other representations.

The other traditional approach is using conventional rule engine (normally production rule engine). Jess is a familiar rule engine and scripting environment written entirely in Sun's java language. Jess gives the capability for building Knowledge in the form of declarative rules and facts, and reason about it. Also Jess can be integrated efficiently with a JADE agent.

In this paper, A comparative study is held between the above two approaches. An example is implemented to show the tools and steps required in each way and to show the expressivity power of the ontology based over the traditional one.

Keywords-component; Java Agent Development Framework (JADE); Web Ontology Language (OWL); Jess; Knowledge Representation; Description Logic (DL).

I. INTRODUCTION

Knowledge Representation (KR) is one of the most important concepts in artificial intelligent. It's aimed is to represent a domain knowledge, and provide a system of logic to enable inference about it. Expressivity is a key parameter in knowledge representation. A more expressive language leads to easier and compacter representation of the knowledge. But more expressive needs more complex algorithms for constructing inferences.

A set of technologies are developed for representing the knowledge, the most familiar is using a rule-based model. In such a model facts represent data and rules formulated to apply logic which enable inference about the facts producing a new one or answering specific queries. Others technologies are developed for KR, including the most promising formal modeling Web Ontology Language (OWL) [17], which introduces a new aspects and features into the modeling of KR [21].

Now, recently, agent-based technologies are become promising means for the development of distributed applications that require operating in heterogeneous system, because they offer a high level abstraction and cope with distribution and interoperability [2]. The Foundation for Intelligent Physical Agents (FIPA) introduce a several documents about the specifications that define an agent system. From its title FIPA preferred agents to acts intelligence and several efforts has been done for the development of intelligent agent architectures. Intelligent agent is preferred incorporate a knowledge representation in its internal architecture and uses it containing theorem to reason about the application domain.

A future trend is to replace OWL/SWRL (Semantic Web Rule Language) knowledge model over traditional rule based system. Several researchers are working towards this. For example, Meech [1] show the difference in features between existing rule engine technologies and OWL/SWRL in applying business rules to design enterprise information systems. Canadas [10] build a tool for the development of rule based applications for the Web based on OWL and SWRL ontologies. Others try to get the efficiency of rule engine in ontology inference by translating OWL logic into Jess rule. Bontas and Mei [5] present OWL2Jess, which is a comprehensive converter tool enabling Jess reasoning over OWL ontologies. Connor [18] uses SWRL Factory mechanism to integrate the Jess rule engine with SWRL editor.

In this paper a behavioral architecture is implemented to build an intelligent agent in JADE platform with two different knowledge models. The first one is based on OWL ontology, the other is by integrating an agent with the rule based engine Jess. An example is implemented in the two ways to show the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

methods and tools used in both cases, and to show strength and weakness in every way.

II. AGENT BASED SYSTEM

There are several definitions for the term "Agent", but all definition agrees that agent is a software component that has the characteristic of being autonomous [2][14]. Agents can communicate with each other in asynchrony way, they can be cooperative to perform a common task, or it can introduce their own services.

Agent architectures are the fundamental mechanisms underlying the autonomous components that support effective behavior in real-world, dynamic and open environments. From beginning, initial efforts focused on the development of intelligent agent architectures [2][14], FIPA develop open specifications, to support interoperability among agents and agent based applications. FIPA give nothing about how to build internal knowledge in an agent, leaving that to the developers. So, we can see different approaches for building intelligent agent in different FIPA complaint agent systems.

Several agent architectures are developed to support intelligent agent [2][14]:

- Reactive architectures are based on a stimulus–response mechanism.
- Belief Desire Intention (BDI): can reason about their actions.
- Behavioral architecture: An agent has several behaviors which executed in sequence or in parallel depending on the task to perform. This architecture is more suitable for used in real applications and our implementations will based on it.

A. *JADE*

The Java Agent Development Framework (JADE) is a platform that provides a middleware layer to facilitate the development of distributed multi-agent systems in compliance with FIPA specifications [12]. JADE have no mechanism for providing intelligence and reasoning capability.

JADE roots to java give it the ability to integrate easily with other java implementation tools, like Jess (rule engine written entirely in JAVA language) and Jena (Java platform for processing semantic web data standards RDF and OWL). Those tools can be used to build knowledge model within an agent and reason over it.

III. ONTOLOGY AND SEMANTIC WEB

Ontology is a term borrowed from philosophy. In the context of knowledge representation, ontology defined as the shared understanding of some domain, which is often conceived as a set of entities, relations, axioms and instances [9]. Ontology based knowledge representation allow for sharing knowledge between different entities, also knowledge can be reused by reusing or building over well defined Web ontologies. Thus such knowledge model will enhance interoperability between different agents in different platforms [9].

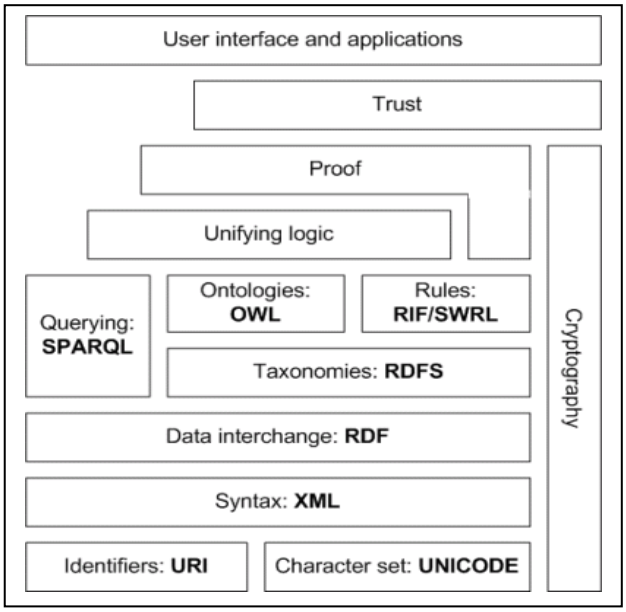


Figure 1. The latest form of Semantic Web stack diagram (W3C Semantic Web Activity, 2008)

The Semantic Web is envisioned as an extension of the current web. According to the World Wide Web Consortium (W3C), "The Semantic Web provides a common framework that allows data to be shared and reused across application, enterprise, and community boundaries" [22].

The main purpose of Semantic Web is to enable users to find their request more efficiently by let machine understand and respond to human request based on their meaning. To let that happen, web resources must be described using a set of W3C standards and technologies to enable its processing. Among these standards are RDF, Schema RDF, and OWL [9].

Fig. 1 shows the Semantic Web diagram as seen by W3C.

IV. WEB ONTOLOGY LANGUAGE

OWL is an ontology language designed for use in the Semantic Web and is the language recommended by the W3C for this use. The OWL language provides three expressive sublanguages, OWL-DL is one of the sublanguage which supports user who wants more expressivity with complete and decidable reasoner. Such languages are based on Description Logic [17].

A. *Description Logic*

Description Logics (DL) are a family of formal knowledge representation languages used to represent ontology based knowledge. The basic syntactic building blocks are concepts (corresponding to classes in object oriented model), roles (represent relationships between two concepts or concept and a data type) and individuals (represent classes instances) [21][4].

The knowledge base in DL consists of a:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- TBox (terminological box): contains a set of axioms which represent the schemas of the knowledge.
- ABox (assertion box): contains all individuals belonging to TBOX classes.

DL have a distinguished feature over other data description formalisms called "Open World Assumption" which means that when knowledge of a fact is not present, this will not imply knowledge of the negation of a fact [21][4].

B. Using OWL-Dl for Building Knowledge Model in jade agent

The first step towards building an ontology based knowledge representation is building the domain specific ontology. Using Protégé editor we can easily model the structure of our knowledge. In OWL, ontology is represented by classes, properties and individuals. Classes represent concepts in domains. OWL has very powerful and expressive way to describe classes [11]:

- Classes can be defined to be disjoined, No individual can be both in two disjoint classes. This will map the disjoint with axiom in DL logic.
- Classes can be described by property restriction. This will map the equivalent axiom in DL logic.
- Classes can be related via a class hierarchy. This will map the subsumption axiom,. This relation said that class B is more general than class A.

The power of expressivity not just in describing classes, but also in defining properties between classes [11]. Properties represent roles in domains:

- Two types of properties: object property which relates an individual to another and data property which relate an individual to data value.
- Property have range and domain (range and domain are not constraints in inference process).
- Property can be defined to be transitive, symmetric or functional. This will give more expressivity to reflect the real world.
- Properties can be related via a property hierarchy.
- Property can be defined to be the inverse of another property (example, greater than is the inverse of small than).

C. Supporting Rules

Normally, decision component encoded in rules, also many business processes are best modeled using a declarative rules [6], so sometimes rules need to be added to OWL knowledge based system.

Semantic Web Rule Language (SWRL) is an expressive OWL-based rule language allowing rules to be expressed in terms of OWL concepts to provide more powerful deductive reasoning capability than OWL alone, coming at the expense of decidability [7]. One should stay within OWL construct until the more expressivity power of SWRL is required.

Also, Jena includes a general purpose rule-based reasoner which support inference over RDF and OWL model and provide forward and backward chaining [8]. Rules in Jana are defined by a JAVA Rule object having the IF...THEN... formalism. Jena rules can be added to OWL model and use Jena rule reasoner as inference on that model.

V. RULE BASED SYSTEM

The idea of rule based system is to represent a domain expert's knowledge in form of rules which represent the logic of the knowledge, always accompanied with facts that represent the data of the knowledge [20]. Another important part of such a system is the rule engine that acts on them. A rule consists of two parts: conditions and actions. The action part might assert a new fact that fire another rules. Rule engine worked by matching available facts with the condition part of the rules, if one matched then its action part will be executed. The architecture of a rule-based system has the following components [19]:

- Rule base: represent the logics as rules that will reason with over data
- Working memory: represent the fact base as facts in knowledge base.
- Inference engine: match a rule to facts in working memory.

A. Jess

Jess is the rule engine for the JAVA platform [23]. One of the most important features of jess is using a rête algorithm to implement its rule engine; this will improve rule-matching performance.

To use Jess for building a knowledge based system, logic is specified in the form of rules using one of the two formats: jess rule language or XML [19]. Also facts can be added for the rules to operate on. When the rule engine is run, a new facts can be added, or any code belong to java can be executed.

Any proposition (as they are used in Propositional Logic) can be represented as a Jess fact. To facilitate reasoning about propositions, predicates are introduced to provide more expressive power. A predicate give a specific property of an object, or express relations between two or more objects.

Jess make the assumption that the system has full knowledge and the absent of facts means that it is false (Closed world Assumption) [10]. This is different from the open world assumption made by owl based knowledge representation.

B. Using JESS for building knowledge model in jade agent

Jess engine can be integrated with jade to build an intelligent agent that act as a decision component. In Jess-JADE integration [16], the intelligence of the agent is handled by Jess. JADE provide the agent communication platform. Using Agent Communication Language (ACL), JADE pass a

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

new knowledge to Jess as a content of ACL message structure. Jess will use its engine to acts upon it.

The implementation of Jess-JADE integration will consists of embedding an instance of Jess engine inside a behavior. A cyclic behavior with action method that consists of running the Jess engine, give the agent the ability to reason continuously [16].

VI. KNOWLEDGE MODEL COMPARISON

A. *Comparison Based in Logic Used*

OWL KR based on DL, while Jess based on propositional and predicate logic. The main strength of DL over other logics is that they offer considerable expressive power going far beyond propositional logic, while reasoning is still decidable. The following expressivity characteristic of OWL- DL over other logics:

- DL supports the transitive relations and can infer about it.
- Support concept hierarchy and property hierarchy.
- Support equivalent axiom that define a new class by descriptions.
- Support cardinality constraint: Number restrictions are sometimes viewed as a Distinguishing feature of DL, Cardinality constraints only supported by some database modeling languages [4].

Rule-Based system in other hand has their strength from the popularity of expressing logic in declarative rules. Most business process has their business rules to work with [1]. Usually user find it more natural to formulate Knowledge in terms of rules than in terms of other kinds of ontological axioms. Rules can often help to express knowledge that cannot be formulated in description logics. At the same time, there are also various features of DL that rule languages do not provide. So one can combined the strengths of DL and rules to get more expressive environment but this comes with the price of more complexity and more difficult implementation [21].

B. *Comparison Based in Inference Engine*

In OWL-DL ontology based knowledge, inference engine will base on DL reasoner, because it can be translated into DL representation. Several popular DL reasoners that are available are listed below:

FaCT++, HermiT, Racer [13] or Pellet.

A description Logic reasoner performs the following inference services:

- Check for concept consistency: A class is inconsistence if it can never have any instances.
- Classify taxonomy: compute inferred hierarchy, find all missing subclass relationship and finding all equivalent classes.
- Compute inferred types.

DL reasoners can inference only on TBOX to find the inconsistency and the super classes for a class. Or inference on just ABOX or in ABOX and TBOX according to the results needs [4].

DL reasoner depends on Tableaux decision procedures [3], while Jess rule engine implements the efficient rete algorithm. Jess is small, single and one of the fastest rule engine [16].

One of the issue to be taken into account is that a JADE agent is single threaded, thus attention should be taken to the reasoner efficiency when integrated with an intelligent agent have interaction with its environment.

VII. EXAMPLE

Our logical problem needs to reason about the shape types depending on its characteristics. A triangle can be defined as a polygon with three sides, where rectangle can be defined as a polygon having four sides.

A. *OWL implementation*

For implementing owl knowledge representation, shape ontology is build using protégé editor. Fig. 2 show a protégé shape ontology graph build using the OntoGraf protégé tab.

Our shape ontology contains two main classes Polygon and Side. Polygon class has 3 subclasses (Rectangle, Triangle, NamedShaped). One object property (hasSide) which shows which Side instances connected to Polygon instance. Two individuals in TBOX:

- RT1 a Polygon instance with 4 hasSide relationship to 4 different Side instances.
- TT1 a Polygon instance with 3 hasSide relationships to 3 different Side instances.

Necessary and sufficient condition is added to Rectangle class which defines Rectangle to be a polygon with 4 hasSide relationship. This constraint is called cardinality constraint supported by OWL-DL based model. Also Triangle can be defined to be a polygon with 3 sides and thus give reasoner a way to recognize the shape type from its characteristic.

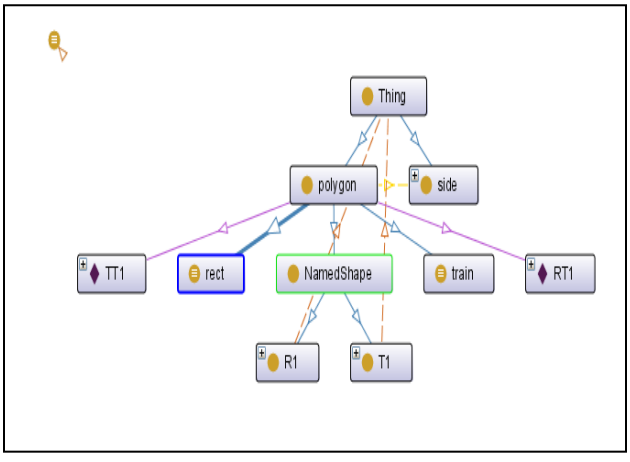


Figure 2. A protégé snapshot of shape ontology graph

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The code for defining rectangle class in turtle format is shown below with the class description:

```
default:rect
    a owl:Class ;
    owl:disjointWith default:train ;
    owl:equivalentClass
    [ a   owl:Class ;
owl:intersectionOf (default:polygon [ a
owl:Restriction ;        owl:cardinality
"4"^^xsd:int ;
          owl:onProperty default:hasSides ])
    ] .
```

Jena Ontology API [8] is used for building and manipulating ontology based knowledge model within the JADE agent. Jena is a free open source Java library for processing semantic web data supporting RDF and OWL data models.

Jena is used to create ontology model through the Jena Model Factory class. Creating ontology model with a memory storage supporting OWL-DL sublanguage as follows:

```
OntModel m= ModelFactory.CreateOntologyModel
(OntModelSpec.OWL_DL_MEM);
```

Reading shape.owl ontology file into the model:

```
m.read("http://www.owl-ontologies.com/shape.owl");
```

Adding inference capability to our model, the following code asks about the instances belongs to class rectangle:

```
Reasoner reasoner = ReasonerRegistry.getOWLReasoner();
// Create ontology model with reasoner support
InfModel inf = ModelFactory.createInfModel(reasoner, m);
OntClass rect = inf.getOntClass(NS + "rect");
ExtendedIterator tt = rect.listInstances( );
 while(tt.hasNext()) {
  OntResource mp = (OntResource)tt.next( );
  System.out.println(mp.getURI( ));   }
```

the result of the above code is:

http://www.owl-ontologies.com/Shape.owl#RT1

which show that RT1 is an individual belong to ontology class rect (Rectangle).

In JADE, agents exchanged messages with each other using ACL. To share knowledge between multiple JADE agents that implements their knowledge in OWL-DL language, JADE should support the OWL-DL Codec so the content of ACL message can be filled with OWL knowledge assertion.

B. Jess implementation:

Taking a look at shape.clp which defines several fact templates:

```
(deftemplate Polygon (slot name) )
(deftemplate Rectangle extends Polygon)
(deftemplate Traingle  extends Polygon)
(deftemplate side(slot code))
 (deftemplate hasSide   (slot name)  (slot code))
```

The keyword extends of the **deftemplate** construct lets you define one template in terms of another. This hierarchical relationship has no influence in reasoning process, just attributes form the above template will be inherited in this template.

Two rules are defined to classify the polygon types. Rules in Jess are defined using **defrule** construct as follows:

```
(defrule find_rect
(Polygon(name ?yy))
(and(side(code ab))(side (code bc))(side (code cd))(side (code da))
(hasSide(name ?yy)(code ?a&ab))
(hasSide(name ?yy)(code ?b&bc))
(hasSide(name ?yy)(code ?c&cd))
(hasSide (name ?yy)(code ?d&da)))
=>
(assert(Rectangle(name ?yy)))
(printout t "assert rectangle  " ?yy crlf);
)

(defrule find_train
(Polygon(name ?yy))
(and(side(code ab))(side (code bc))(side (code ca))
(hasSide(name ?yy)(code ?a&ab))
(hasSide(name ?yy)(code ?b&bc))
(hasSide(name ?yy)(code ?c&ca)))
=>
(assert(Traingle(name ?yy)))
(printout t "assert traingle  " ?yy crlf);
)
```

In jess, no cardinality constraint can be specified leading to less expressivity in defining the logic. Thus Jess rules to recognize the shape types are more specific and less expressive.

To integrate with JADE: Adding Jess behavior to the Setup method of jade Agent will let agent access an instance of Jess engine. Then Jess-Jade agent can be used as a decision component for this domain knowledge.

The result for applying the above code is

```
==>f-0 (MAIN::initial-fact)
==>f-1(MAIN::MyAgent   (nametest@192.168.68.4:1099/JADE))
==> f-2 (MAIN::Polygon (name t1))
==> f-3 (MAIN::Polygon (name t2))
==> f-4 (MAIN::hasSide (name t1) (code ab))
==> f-5 (MAIN::hasSide (name t1) (code bc))
==> f-6 (MAIN::hasSide (name t1) (code ca))
==> f-7 (MAIN::hasSide (name t2) (code ab))
```


http://sites.google.com/site/ijcsis/
ISSN 1947-5500

==> f-8 (MAIN::hasSide (name t2) (code bc))

==> f-9 (MAIN::hasSide (name t2) (code cd))

==> f-10 (MAIN::hasSide (name t2) (code da))

==> f-11 (MAIN::Rectangle (name t2))

==> f-12 (MAIN::Traingle (name t1))

Jess agent can assert and retract Jess facts during runtime. These assertion or retraction can be a decision of other environmental agents that can be communicate and share knowledge using ACL language. To support this communication a JADE ontology is build called jshape which define the concepts (polygon, triangle, rectangle, side), predicate (hasSide) and Action elements (assert and retract) for adding and deleting actions.

Using jshape ontology and semantic language for the message content, the following ACL message will assert a new fact that adds t3 as a new polygon in our knowledge base:

{Request

:sender (agent-identifier

:name WorkAgent@localhost:1099/JADE

:addresses (sequence http://localhost:7778/acc))

:receiver (set (agent-identifier :name JessAgent@localhost:1099/JADE))

:content

(agent-identifier :name WorkAgent@localhost:1099/JADE)

((action

(assert

(Polygon :name "t3"))

:language SL

:ontology http://myontology.jshape))

}

VIII. CONCLUSION

In this paper, we try to show some of the main differences between using OWL–DL language and Jess rule engine to build an intelligent JADE agent. We can summarize those differences as follows:

- OWL is more expressive than facts and rules structure, rules are more familiar to used.
- Rules are closer to simulate a decision component; OWL may need to add some rules to behave as a decision component.
- OWL ontology model is closer to Object-Oriented Model. This will facilitate building knowledge from existing object oriented models.
- Knowledge in OWL can easily expanded and builds over it, because it well formed and structured. Jess knowledge always restricted to solve a particular problem and a new problem needs a new knowledge.
- Because of the high expressivity of OWL model, Reasoned on large ontologies has the efficiency problem, Jess rule engine is small and light and more efficient.
- OWL is W3C standard thus support interoperability between different platforms, Jess rule based system has limited support for interoperability.
- Supporting knowledge sharing between agents in OWL needs OWL and RDF codec to be supported as content for ACL message. Jess may use strings in sending and receiving knowledge.

REFERENCES

[1] A. Meech, "Business Rules Using OWL and SWRL ," Advanced in Semantic Computing, Vol. 2, pp. 23-31, 2010

[2] F. Bellifemine, G. Caire, D. Greenwood, Developing Multi-Agent Systems with JADE. John Wily & Sons, Ltd, 2007.

[3] F. Baader, U. Sattler, An overview of tableau algorithms for description logics, Studia Logica, 69(1), pp 5-40. Springer.

[4] F. Baader, Description Logic handbook :Theory, Implementation, & Applications, Cambridg University Press New York, NY, USA, 2003.

[5] J. Mei, E. Bontas, "Reasoning Paradigms for OWL Ontologies," Univ. of Berlin, Tech. Rep. B-04-12, Nov. 2004.

[6] M. O'Connor, H. Knublauch, S. Tu, B. Grosof, M. Dean, W. Grosso, M. Musen, "Supporting Rule System Interoperability on the Semantic Web with SWRL," In Proc. International Semantic Web Conference, 2005 .pp 974-986.

[7] Protégé Web Site [Online]. Available: http://protege.cim3.net/

[8] Jena Web Site [Online]. Available: http://jena.apache.org/

[9] D.Q. Zhang, T. Gu, H.K. Pung, Ontology Based Context Modeling and Reasoning using OWL. In Proc. Second IEEE Annual Conference, March 2004, p. 18-22.

[10] J. Cañadas, J. Palma, S. Túnez,, "A Tool for MDD of Rule-based Web Applications based on OWL and SWRL," In Proc. 6th Workshop on Knowledge Engineering and Software Engineering, 2010

[11] I. Horrocks, P. Patel-Schneider, Knowledge Representation and Reasoning on the Semantic Web: OWL In Handbook of Semantic Web Technologies. Ist Ed., Springer. 2011, ISBN 978-3-540-92912-3.

[12] A. LUPAŞC, A multi agent platform for developments of Accounting Intelligent Applications. annuals of "Dunares de jos", University of Galati, Fascicle1- Economics and Applied informatics, 2008.

[13] Racer Web Site [Online]. Available :http://www.sts.tu-harburg.de/~r.f.moeller/racer/.

[14] M. Laclavik, "Ontology and Agent based Approach for Knowledge Management," Phd. Thesis, Institute of Informatics. Slovak Academy of Science, June 2005.

[15] M. Rashid, "Diagrammatic Representation of OWL Ontologies." M.Sc. thesis, Free University of BOZEN-BOLZANO, March 2009.

[16] H. Cardoso, (2007) Integrating JADE and Jess. University of Porto [Online] . Available: http://jade.tilab.com/doc/tutorials/jade-jess.

[17] (2009) W3C OWL Working Group: OWL 2 Web Ontology Language: Document Overview. W3C Recommendation Available : http://www.w3.org/TR/owl2-overview/

[18] M. O'Connor, H. Knublauch, S. Tu,, B. Grosof,, M. Dean, W. Grosso, M. Musen, "Supporting Rule System Interoperability on the Semantic Web with SWRL," In proc. ISWC2005 2005.

[19] J. Joël Vogt, "Jess to JADE Toolkit (J2J) A Rule-Based Solution Supporting Intelligent and Adaptive Agents," M.Sc. thesis. Software Engineering Group, Department of Informatics, University of Fribourg, Switzerland, aug. 2008

[20] C. Wu, (2004) Modeling Rule-Based System with EMF. [Online] Available : http://www.eclipse.org/articles

[21] Krötzsch, M. Description Logic Rules. M.Sc. thesis. Tag der mündlichen Prüfung: Februar 2010

[22] T. Berners-Lee, J. Hendler, and O. Lassila, ,(2001), The Semantic Web, Scientific American, May 2001, p.28-37.

[23] JessWeb Site [Online]. Available: http://www.jessrules.com/

Modeling and Control of CSTR using Model based Neural Network Predictive Control

Piyush Shrivastava
Assistant Professor,
Electrical& Electronics EngineeringDepartment,
Takshshila Institute of Engineering & Technology,
Jabalpur, Madhya Pradesh, India

***Abstract*—this paper presents a predictive control strategy based on neural network model of the plant is applied to Continuous Stirred Tank Reactor (CSTR). This system is a highly nonlinear process; therefore, a nonlinear predictive method, e.g., neural network predictive control, can be a better match to govern the system dynamics. In the paper, the NN model and the way in which it can be used to predict the behavior of the CSTR process over a certain prediction horizon are described, and some comments about the optimization procedure are made. Predictive control algorithm is applied to control the concentration in a continuous stirred tank reactor (CSTR), whose parameters are optimally determined by solving quadratic performance index using the optimization algorithm. An efficient control of the product concentration in cstr can be achieved only through accurate model. Here an attempt is made to alleviate the modeling difficulties using Artificial Intelligent technique such as Neural Network. Simulation results demonstrate the feasibility and effectiveness of the NNMPC technique.**

Keywords-Continuous Stirred Tank Reactor; Neural Network based Predictive Control; Nonlinear Auto Regressive with eXogenous signal.

I. INTRODUCTION

One of the main aims in industry is to reduce operating costs. This implies improvements in the final product quality, as well as making better use of the energy resources. Advanced control systems are in fact designed to cope with these requirements. Model based predictive control (MBPC) [1,2] is now widely used in industry and a large number of implementation algorithms due to its ability to handle difficult control problems which involve multivariable process interactions, constraints in the system variables, time delays, etc. The most important advantage of the MPC technology comes from the process model itself, which allows the controller to deal with an exact replica of the real process dynamics, implying a much better control quality. The inclusion of the constraints is the feature that most clearly distinguishes MPC from other process control techniques, leading to a tighter control and a more reliable controller.

Another important characteristic, which contributes to the success of the MPC technique, is that the MPC algorithms consider plant behavior over a future horizon in time. Thus, the effects of both feedforward and feedback disturbances can be anticipated and eliminated, fact which permits the controller to drive the process output more closely to the reference trajectory. The classical MBPC algorithms use linear models of the process to predict the output of the process over a certain horizon, and to evaluate a future sequence of control signals in order to minimize a certain cost function that takes account of the future output prediction errors over a reference trajectory, as well as control efforts. Although industrial processes especially continuous and batch processes in chemical and petrochemical plants usually contain complex nonlinearities, most of the MPC algorithms are based on a linear model of the process and such predictive control algorithms may not give rise to satisfactory control performance [3, 4]. Linear models such as step response and impulse response models are preferred, because they can be identified in a straightforward manner from process test data. In addition, the goal for most of the applications is to maintain the system at a desired steady state, rather than moving rapidly between different operating points, so a precisely identified linear model is sufficiently accurate in the neighborhood of a single operating point. As linear models are reliable from this point of view, they will provide most of the benefits with MPC technology. Even so, if the process is highly nonlinear and subject to large frequent disturbances; a nonlinear model will be necessary to describe the behavior of the process. Also in servo control problems where the operating point is frequently changing, a nonlinear model of the plant is indispensable. In situations like the ones mentioned above, the task of obtaining a high-fidelity model is more difficult to build for nonlinear processes.

In recent years, the use of neural networks for nonlinear system identification has proved to be extremely successful [5-9]. The aim of this paper is to develop a nonlinear control technique to provide high-quality control in the presence of nonlinearities, as well as a better understanding of the design process when using these emerging technologies, i.e., neural network control algorithm. The combination of neural networks and model-based predictive control seems to be a good choice to achieve good performance in the control. In this paper, we will use an optimization algorithm to minimize the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

cost function and obtain the control input. The paper analyses a neural network based nonlinear predictive controller for a Continuous Stirred Tank Reactor (CSTR), which is a highly nonlinear process. The procedure is based on construction of a neural model for the process and the proper use of that in the optimization process.

This paper begins with an introduction about the predictive control and then the description of the nonlinear predictive control and the way in which it is implemented. The neural model and the way in which it can be used to predict the behavior of the CSTR process over a certain prediction horizon are described, and some comments about the optimization procedure are made. Afterwards, the control aims, the steps in the design of the control system, and some simulation results are discussed.

II. PREDICTIVE CONTROL

The predictive controller, in summary, is characterized by computing future control actions based on output values predicted by a model, with vast literature and academic and industrial interest (Clarke, 1987; Garcia et all, 1989; Arnaldo, 1998) [4]. This section presents the concepts of predictive control based on NPC, using the usual optimization functions and control laws, applied to the conventional predictive controllers.

A. Optimization functions

The optimization function, usually represented by the index J, represents the function that the control action tries to minimize. In an intuitive way, the error between the plant output and the desired value is the simplest example of an optimization function, and it is expressed by:

$$J = y_{ref}(k) - y(k) = e(k) \quad (1)$$

Where:
$y(k)$ represent the plant output
$y\ k\ ref\ (\)$represent the desired response
$e(k)$ represent the estimation error
k is the sample time

One of the most usual optimization functions is based on the square error and it is represented as:

$$J = \left[y_{ref}(k) - y(k)\right]^2 = \left[e(k)\right]^2 \quad (2)$$

But the optimization index can take forms of more complex functions. For predictive controllers, whose models are capable to predict N steps ahead, the simple application of the square error approach can present satisfactory results. This case admits that the optimization function is not limited to an only point, but an entire vector of N predicted errors. It seeks to optimize the whole trajectory of the future control actions in a horizon of N steps ahead.

$$J = \sum_{j=1}^{N}\left[y_{ref}(k+j) - \hat{y}(k+j)\right]^2 = \sum_{j=1}^{N}\left[e(k+j)\right]^2 \quad (3)$$

More complex optimization functions can consider the control effort. It is the specific case of GPC (Generalized Predictive Control), where the optimization index J can be expressed as:

$$J = \sum_{j=N_1}^{N_Y}\left[y_{ref}(k+j) - \hat{y}(k+j)\right]^2 + \sum_{j=1}^{N_U}\alpha(j).\left[\Delta u(k+j)\right]^2 \quad (4)$$

where:
$y(k)$ - is the output plant estimation at instant = k
Δu - is the control action increment.
N_1 - is the minimum horizon of prediction.
N_U - is the control horizon.
N_Y - is the maximum horizon of prediction.

The objective of the control problem is to minimize the index J, with respect to the control actions, looking for the points where the first order differential is null.

III. NEURAL NETWORK PREDICTIVE CONTROL

By the knowledge of the identified neural model of the nonlinear plant which is capable of doing multi step ahead predictions, Predictive control algorithm is applied to control nonlinear process. The idea of predictive control is to minimize cost function, J at each sampling point:

$$J(t,U(k)) = \sum_{i=N_1}^{N_2}\left[r(k+i) - \hat{y}(k+i)\right]^2 + \sum_{i=1}^{N_u}\rho\left[\Delta u(k+i-1)\right]^2 \quad (5)$$

With respect to the N_u future controls,

$$U(k) = [u(k).....u(k+N_u-1)]^T \quad (6)$$

and subject to constraints:

$$N_u \le i \le (N_2 - n_k) \quad (7)$$

Using the predictive control strategy with identified NARX model (NNMPC) it is possible to calculate the optimal control sequence for nonlinear plant. Here, term $r(k+i)$ is the required reference plant output, $\hat{y}(k+i)$ is predicted NN model output, $\Delta u(k+i-1)$ is the control increment, N_1 and N_2 are the minimum and maximum prediction (or cost) horizons, Nu is the control horizon, and ρ is the control penalty factor[4].

The predictive control approach is also termed as a receding horizon strategy, as it solves the above-defined optimization problem [5] for a finite future, at a current time and implements the first optimal control input as the current control input. The vector $u = [\Delta u(k), \Delta u(k+1), \ldots \Delta u(k+Nu-1)]$ is calculated by minimizing cost function, J at each sample k for selected values of the control parameters $\{N_1, N_2, Nu, \rho\}$.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

These control parameters defines the predictive control performance. N_1 is usually set to a value 1 that is equal to the time delay, and N_2is set to define the prediction horizon i.e. the number of time-steps in the future for which the plant response is recursively predicted.

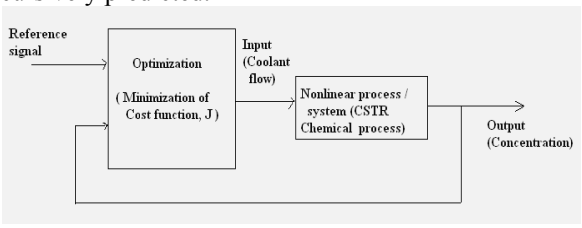


Figure 1: NNMPC principle applied to CSTR chemical process

The minimization of criterion, *J* in NNMPCis an optimization problem minimized iteratively. Similar to NN training strategies, iterative search methods are applied to determine the minimum.

$$\theta^{(i+1)}=\theta^{(i)}+\mu^{(i)}.d^{(i)} \quad (8)$$

where, $\theta^{(i)}$ specifies the current iterate (number 'i'), $d^{(i)}$ is the search direction and $\mu^{(i)}$ is the step size. Various types of algorithms exist, characterized by the way in which search direction and step size are selected. In the present work Newton based Levenberg–Marquardt (LM) algorithm is implemented. The search direction applied in LM algorithm is:

$$(\hat{H}[U^i(t)]+\lambda^i I)d^i = -G[U^i(t)] \quad (9)$$

with Gradient vector and Hessian matrix as:

$$G[U^i(t)] = \frac{\partial J(t,U(t))}{\partial U(t)}\Big|_{U(t)=U^i(t)}$$

$$= -2\varphi^T[U^i(t)]\tilde{E}(t)+2\rho\frac{\partial\tilde{U}(t)}{\partial U(t)}\tilde{U}(t)\Big|_{U(t)=U^i(t)} \quad (10)$$

$$H[U^i(t)] = \frac{\partial^2 J(t,\tilde{U}(t))}{\partial U(t)^2}\Big|_{U(t)=U^i(t)}$$

$$=\frac{\partial}{\partial U(t)}\left(\frac{\partial\hat{Y}(t)}{\partial U(t)}E(t)\right)+2\rho\frac{\partial\tilde{U}^T(t)}{\partial U(t)}\frac{\partial\tilde{U}(t)}{\partial U(t)}\Big|_{U(t)=U^i(t)} \quad (11)$$

where $B^{(i)}$ specifies the approximation of the inverse Hessian and $G[U^{(i)}(t)]$ is the gradient of the *J* with respect to the control inputs. The most popular formula known as Broyden-Fletcher-Goldfarb-Shanno (BFGS) algorithm to approximate the inverse Hessian is used here[8]. The proposed scheme of implementing the NNMPC is shown in Figure 2.

Time Series Prediction with Neural Networks

The purpose of our neural network model is to do time series prediction of the plant output. Given a series of control signals $\tilde{u}$ and past data y_t it is desired to predict the plant output series y_N.The network is trained to do *one step ahead* prediction[9], i.e. to predict the plant output y_{t+1} given the current control signal u_t and plant output y_t . The neural network will implement the function

$$\hat{y}_{t+1} = f(u_t, y_t) \quad (12)$$

As it is discussed above, y_t has to contain sufficient information for this prediction to be possible.It is assumed that y_t is multivariable. One problem is that this method will cause a rapidly increasing divergence due to accumulation of errors. It therefore puts high demands on accuracy of the model. The better the model matches the actual plant the less significant the accumulated error. A sampling time as large as possible is an effective method to reduce the error accumulation as it effectively reduces the number of steps needed for a given time horizon. The neural network trained to do one step ahead prediction will model the plant. The acquisition of this model is also referred to as System Identification.

IV. Modeling of Neural Network Predictive Control (NNPC)

The three steps involved in the ANN model development are

A. Generation of Input-Output data

The data generated to train the network should contain all the relevant information about the dynamics of the CSTR. The input was given to the conventional model of the CSTR and from the conventional model, the input and output were sampled for 0.02 sampling instants and the required sampled data are obtained to train the network.

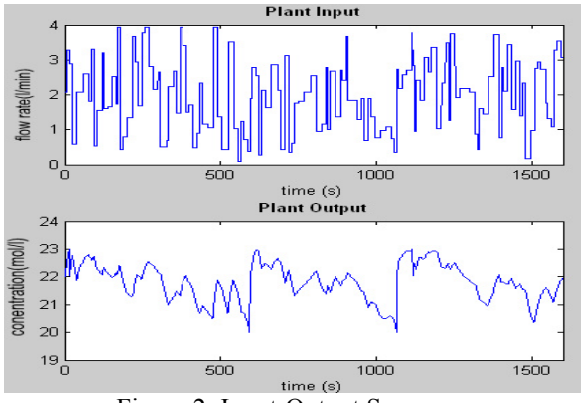


Figure 2: Input-Output Sequence

B. Neural Network Architecture

The feed forward network with sigmoidal activation function was chosen based on the trials with different structures of multilayer perceptron.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

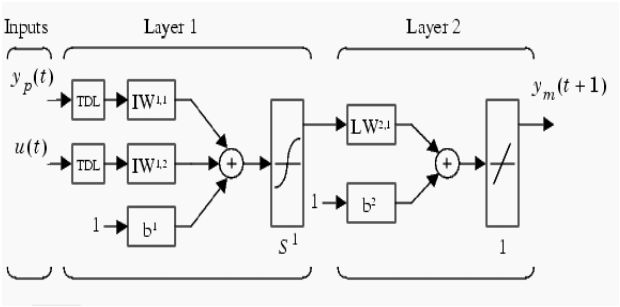


Figure 3: ANN model of the CSTR

The lowest error corresponds to 7 neurons in the hidden layer. Hence it is selected as optimal architecture of ANN. The ANN selected here consists of 4 neurons in the input layer, 7 neurons in the hidden layer and one neuron in the output layer. The ANN architecture used in the present work is shown in Figure 3. The training algorithm used in the CSTR modeling is back propagation algorithm. Before training the process weights are initialized to small random numbers. The weights are adjusted till error gets minimized for all training sets. When the error for the entire set is acceptably low, the training is stopped.

Table 2 shows the parameters used in developing the ANN model for the CSTR

Parameters	***Values***
Input neurons	4
Output Neurons	1
Hidden layer Neurons	7
No. of hidden layer	7
Activation function	Sigmoidal
Training algorithm	Levenberg-Marquardt
Iteration	10000
Architecture	Feedforward
Initial weights	1

Table 2: ANN Parameters for CSTR modeling

C. Model Validation

The final step in developing the model is validation of the model [11]. Validation is performed by evaluating the model performance using trained data and test data. The input and target were presented to the network and the network was trained using Levenberg-Marquardt algorithm.

Validation tests on training set:

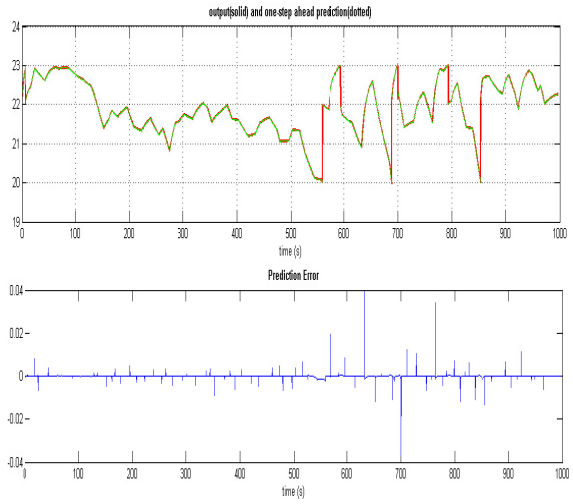


Figure 4: (a) One step ahead prediction of model, (b) Prediction error between model output and predicted output

Validation tests on test set:

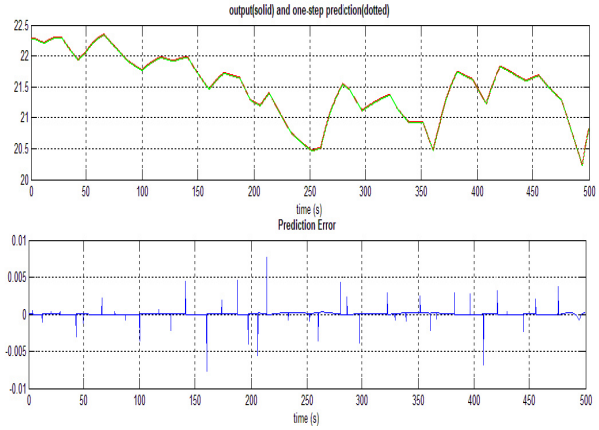


Figure 5 :(a) one step ahead prediction of model (validation set), (b) Prediction error between model output and predicted output (validation set)

V. CONTINUOUS STIRRED TANK REACTOR

The Continuous Stirred Tank Reactor [6] is shown in Figure 6.This CSTR model in used as the nonlinear system.

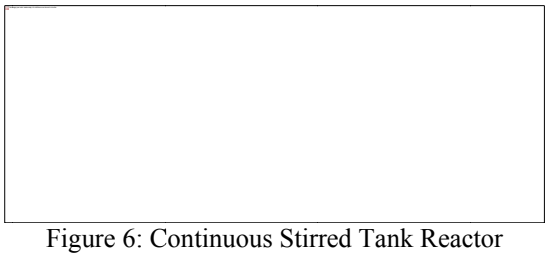


Figure 6: Continuous Stirred Tank Reactor

The equations which shows the dynamic model of the system is

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

$$\frac{dh(t)}{dt} = w_1(t) + w_2(t) - 0.2\sqrt{h(t)} \quad (14)$$

$$\frac{dC_b(t)}{dt} = (C_{b1} - C_b(t))\frac{w_1(t)}{h(t)} + (C_{b2} - C_b(t))\frac{w_2(t)}{h(t)} - \frac{k_1 C_b(t)}{(1 + k_2 C_b(t))^2} \quad (15)$$

where h (t) is the liquid level, $C_b(t)$ is the product concentration at the output of the process, $w_1(t)$ is the flow rate of the concentrated feed C_{b1} and $w_2(t)$ is the flow rate of the diluted feed C_{b2} .The input concentration are set to C_{b1}=24.9 and C_{b2}= 0.1.The constants associated with the rate of consumption are k_1=k_2=1.

The objective of the controller is to maintain the product concentration by adjusting the flow w_1 (t), w_2 (t) =0.1.The level of the tank h is not controlled. The designed controller uses a neural network model to predict future CSTR responses to potential control signals. The training data were obtained from the nonlinear model of CSTR.

VI. Simulation Results and Conclusion

The objective of the control strategy is to govern theCSTR dynamics to force the system concentration to track a certain set-points. In this system, the input is the coolant flow rate and the output is the concentration of the process [12]. The identifier is trained and initialized before the control action starts. The input vector of the identifier includes coolant flow rates at different time steps (the sampling time is 20sec).
The performance of the proposed controller is shown in Figure 7. Evidently, the concentration values of the plant could track the set-point values excellent. It is to be noted that to improve the transient response, one may consider a larger prediction time. It is remarkable to note that because of highly nonlinearity nature of CSTR process, using the conventional control technique could not reach the control task. It can be seen in figure 7 that controller output is tracking the reference signal.

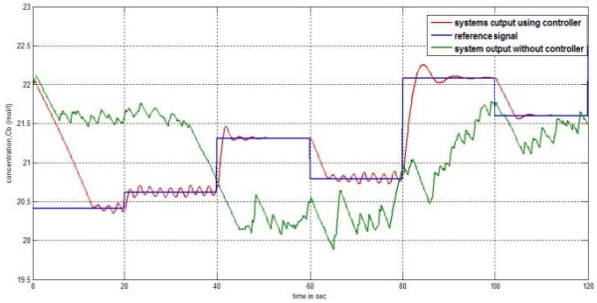


Figure 7: Response graph with and without controller

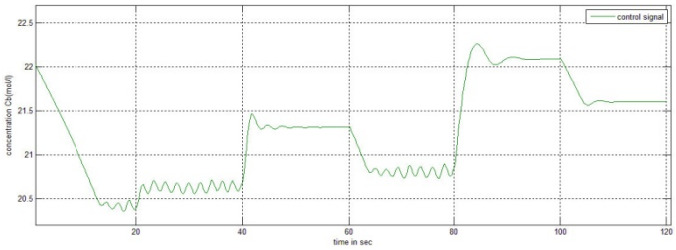


Figure 8: control signal by the controller

In this paper modeling of CSTR has been implemented using artificial neural networks. The neural model has been trained using data set obtained from dynamic equations. Feed forward neural network has been used to model the CSTR. The neural model has been designed as a black box model. The simulation results from conventional model and the neural model were compared for the given input variations and the results have been found satisfactory. The simulation shows that implementation of the Neural Network based advanced controllers for the set-point tracking case were able to force process output variables to their target values smoothly and within reasonable rise and settling times.

VII. References

[1] Garcia C. E. and Morari, M. 1982. Internal model control-I. “A unifying review and some new results,Industrial Engineering Chemical Process ”. Dev. 21, 308--323.

[2] L.G. Lightbody and G. W. Irwin, “Neural networks for nonlinear adaptive control, “in Proc. IFAC Symp. Algorithms Architectures Real-Time Control, Bangor, U.K. pp. 1–13, 1992.

[3] D. W. Clarke, C. Mohtadi and P. S. Tuffs, “Generalized Predictive Control Basic Algorithm”, Automatica, Vol.23, no.2, pp: 137- 148, 1987.

[4] Morari, M. and Lee, J. H. 1999. Model predictive control: past, present and future, Computers and Chemical Engineering, 23, 667-682.

[5] X. Zhu, D.E. Seborg, “Nonlinear model predictive control based on Hammerstein models”, in. Proc. International Symposium on Process System Engineering, Seoul, Korea, pp. 995–1000, 1994.

[6] Vasičkaninova and M. Bakošova, “Neural network predictive control of a chemical reactor” Proceedings 23rd European Conference on Modelling and Simulation ©ECMS Javier Otamendi, Andrzej Bargiela, 2006.

[7] J. D. Morningred, B. E. Paden, D. E. Seborg, and D. A. Mellichamp, “An adaptive nonlinear predictive controller,” in Proc. Amer. Control Conference., vol. 2,,pp. 1614–1619,1990.

[8] N. Kishor, “Nonlinear predictive control to track deviated power of an identified NNARX model of a hydro plant”. Expert Systems with Applications 35, 1741–1751, 2008.

[9] Tan, Y. and Cauwenberghe, A. “Non-linear one step ahead control using neural networks: control strategy and

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

stability design", Automatica, vol 32, no. 12, 1701-1706, 1996.

[10] Dan, W.P., 1996. Artificial Neural Networks- Theory and Applications. Prentice Hall, Upper Saddle River, New Jersey, USA.

[11] S.A.Billings, and W.S.F. Voon, "Correlation based model validity tests for nonlinear models. International Journal of Control, 44, 235–244.1986.

AUTHORS PROFILE

Author is presently working as Assistant Professor in Electrical and Electronics Department of Takshshila Institute of Engineering and Technology. He received the Masters degree in Electrical Engineering with specialization in Control Systems Engineering from Jabalpur Engineering College. His area of specialization is in Neural Networks, Control Systems, Fuzzy Logic.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Visualization for Levels of Animals Diseases by Integrating OLAP and GIS

Hesham Ahmed Hassan
Faculty of Computer and Information,
Cairo University
Giza, Egypt

Hazem El-Bakry
Faculty of Computer and Information,
Sciences, Mansoura University
Mansoura, Egypt

Hamada Gaber Abd Allah
Faculty of Computer and Information,
Sciences, Mansoura University
Mansoura, Egypt

Abstract

Animal diseases have constituted a major problem in many developing and developed countries. There are different limitations for the existing computer systems to meet the required information and analytical capabilities for a better decision in the Egyptian animal production domain. This paper presents an approach for helping policy/decision makers to improve animal production in Egypt. The paper integrates Online Analytical Processing (OLAP), Geographical Information System (GIS), Spatial Analysis functions and Multicriteria Decision Analysis (MCDA) capabilities to develop a Spatial Decision Support System (SDSS). The main aim of this study is to generate a composite map for decision makers by using some effective factors affect animal production in Egypt. We visualize and analyze different factors such as "*Diseases*", "*Climate*", "*Soil Pollution*", "*Veterinary care*" and "*Economical factors*" which affect the animal production in Egypt. The paper takes in consideration influence of each factor because importance and influence of each factor differs according policy/decision makers point of view.

Keywords: *Geographical Information System (GIS), Multicriteria Decision Analysis (MCDA), Online Analytical Processing (OLAP), Spatial Analysis and Spatial Decision Support System (SDSS).*

1. Introduction

Food crises in less-developed countries have been noted to be the main obstacle to economic development. Moreover, feeding adequately a population growing at an annual rate of 2.1 %, with limited land and water resources, is considered the most important challenge for Egypt. The population of 74 million is expected to rise to 90 million by the year 2017. The high population growth rate is a major constraint for sustainable development in Egypt. In Egypt the population dynamics tells interesting situation: dairy cattle -5.3%, buffaloes +12.1%, beef cattle +50.0%, sheep +29.9%, goats +32.8%, while people numbers increased more than 18%. Nevertheless, there is a shortage of protein and calcium from animal sources produced in Egypt in comparison to nutritional requirements, and there is an increasing gap between dairy products produced domestically and the amount consumed. The gap between domestic animal production and consumption has been estimated at an average of 17 per cent for red meat and 19 per cent for milk. This gap has been continuously widening over recent years and consequently dependence on food imports has been increasing [1]. In 2000 population of dairy animals in Egypt was about 6.7 million heads of cattle and buffaloes contributing about 30% of the total value of agricultural production. [2].

The agricultural domain in Egypt plays a crucial role in the national economy as it represents 20% of GDP and employs nearly 30% of the working population. Also, the feeding adequately a population growing at an annual rate of 1.8%, with limited water resources and land, is considered as the most important challenge for policy makers in Egypt. In addition, the national food security has been noted to be the main goal to achieve a real development and to meet rising of the Egyptian population that expected to be more than 100 million by the year 2030. The policy/decision makers' strategy for animal production in Egypt, up to year 2037, aims to reduce the milk production gap to be less than 10% [3].

Geographical Information System (GIS) links a location and attribute information and enables a person to visualize patterns, relationships, and trends. This process gives an entirely new perspective to data analysis that cannot be easily seen in a table or list format or on a paper map. Exploring data using GIS turns data into information into knowledge. There are two ways that the layers of location can be visualized on a map: Raster layers are organized in a grid of identically sized cells. The cells have a uniform length and width (square shaped) and are called "pixels." Vector layers are represented as points, lines, or polygons. A vector layer cannot mix types together. One layer cannot have both points and polygons. The layer would have to be split into two separate layers; one for points and one for polygons. Vector data is used when the features have specific locations and boundaries and the attribute data is

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

uniform throughout the individual features. Examples of vector layers include bus stops (point), roads (line), and counties (polygon).

Transactional systems are not designed to support the decisional processes, new types of systems have been developed to specifically fulfill decisional needs; they are called “Analytical Systems” and are known on the market as “Business Intelligence” (BI) solutions. In the BI world, data warehouses are based on data structures called “multidimensional”. The term “multidimensional” was coined in the mid-1980s by the community of computer scientists who were involved in the extraction of meaningful information from very large statistical databases (ex. national census). The most widely used BI solutions are OLAP (On-Line Analytical Processing) systems, which provide a unique capability to interactively explore the data warehouse. OLAP technology is based on the multidimensional database approach, which introduces concepts that differ from the concepts found in the transactional database approach. The key multidimensional concepts include: dimensions, members, measures, facts and data cubes [4]. A cube is a multidimensional structure that contains dimensions and measures. Dimensions define the structure of the cube, and measures provide the numerical values of interest to the end user.

OLAP systems are expected to [5]:

- Provide ad hoc access.
- Support the complex analysis requirements of decision-makers.
- Analyze the data from a number of different perspectives (business dimensions).
- Support complex analyses against large input (atomic-level) datasets.

In order to improve the efficiency and response time of the Data Warehouse, the preferred structure is the Star Schema. Star Schemas a database structure in which data is maintained in a single fact table located at the center of the schema with additional dimension data stored in dimensional tables, with all hierarchies collapsed.

Decision makers have turned to analysts and analytical modeling techniques to enhance their decision making capabilities. Spatial decision support systems (SDSS) are explicitly designed to support a decision research process for complex spatial problems. SDSS provide a framework for integrating database management systems with analytical models, graphical display and tabular reporting capabilities, and the export knowledge of decision makers. Such systems can be viewed as spatial analogues of decision support systems (DSS) developed in operational research and management science to address business problems [6].

What really makes the difference between a SDSS (Spatial Decision Support System) and a traditional DSS (Decision Support System) is the particular nature of the geographic data considered in different spatial problems. In addition, traditional DSSs are devoted almost only to solve structured and simple problems which make them non practicable for complex spatial problems [7]. SDSS requires the addition of a range of specific techniques and functionalities used especially to manage spatial data, to conventional DSSs. These additional capacities enable the SDSS to [6];

- acquire and manage the spatial data,
- represent the structure of geographical objects and their spatial relations,
- diffuse the results of the user queries and SDSS analysis according to different spatial forms including maps, graphs, etc., and to
- Perform an effective spatial analysis by the use of specific techniques.

Multi-criteria decision making (MCDM) refers to making decisions for alternatives in the presence of multiple and conflicting criteria. A main contribution area of MCDM is making preference decision (e.g., evaluation, prioritization, selection) over the available alternatives such as a set of products that are characterized by multiple, usually conflicting attributes [8].

2. Problem Formulation

The Central Laboratory for Agriculture Expert Systems (CLAES) in Egypt hosts the data base of Bovine Information System (BOVIS) project that has more than 2 million records represented in 52 tables. In this paper we use El Sharkeya Governorate as case study. [2]Tables related to cow or buffalo sex, major disease categories, various diseases and disorders that affect them, the breeds, the governorate, directorates and the veterinary units they are affiliated to were classified for mining. As data production and collection is escalating.

The purpose of this paper is to do the following:

1. Building OLAP (Online Analytical Processing) system instead of TPS (Transaction Processing System).
2. Visualizing OLAP output dimensions using Geographical Information System (GIS).
3. Using GIS Spatial Analysis capabilities.
4. Building Spatial Multiple Criteria Decision Analysis for different factors diseases, Climate, Soil pollution and Economical factor see Fig (1).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

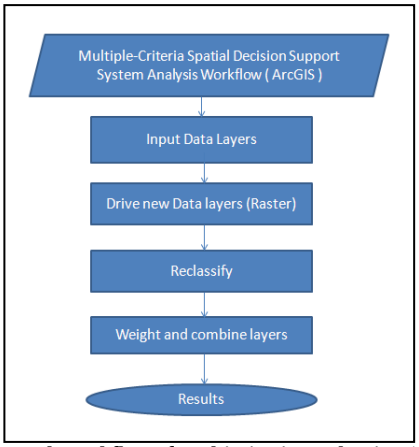


Fig 1. General Workflow of Multicriteria Evaluation (MCE)

3. Proposed Method

3.1 Building OLAP Database

There is an existing OLAP database for BOVIS project build by CLAES team. OLAP see BOVIS from different dimensions such as animal count, deaths, disorders/disease, and pregnancy …etc Fig (2).



Fig 2. BOVIS OLAP Cubes and Dimensions

An OLAP system is built especially to navigate within multidimensional cubes, i.e., to go from one fact to another in an interactive manner and to obtain fast responses. We visualize OLAP multidimensional cubes using Web based Dundas OLAP services and ASP.Net see Fig (3).

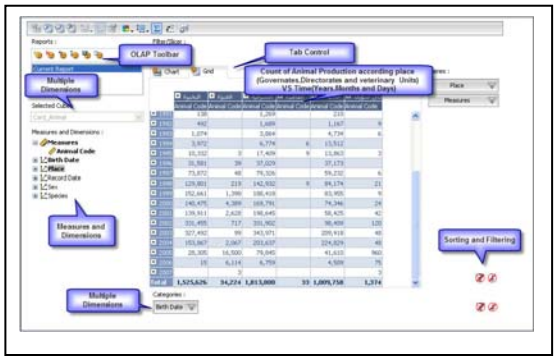


Fig 3. a: Web-Based OLAP Dundas Visualization (Grid)

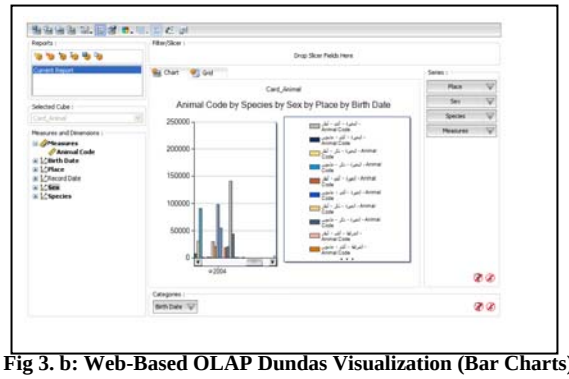


Fig 3. b: Web-Based OLAP Dundas Visualization (Bar Charts)

Web Based Dundas tool allows users to select dynamic cubes and determine measures and dimensions. Users can choose any cube such as "*card_animal*", "*death*"," *disorder*", "*pregnancy*", *"slaughters*", "*vaccine*" …etc (see Fig 2). Also users can specify way of display data either Grid or Bar Charts.

3.2 Visualizing OLAP Output Dimensions

In these step we use GIS engine to visualize OLAP dimensions by preparing data in ArcCatalog GIS using feature classes and relationship class for El Sharkeya governorate.

Feature classes are homogeneous collections of common features, each having the same spatial representation, such as points, lines, or polygons, and a common set of attribute columns see Fig (4).

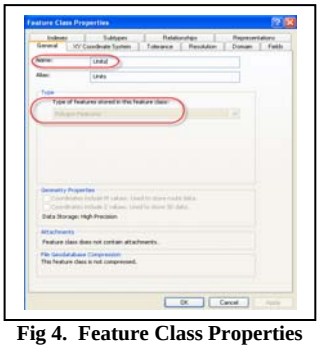


Fig 4. Feature Class Properties

Three layers namely: *"Veterinary Units*", "*Climate*" and "*Economical Standard of Living*" are represented as Polygon feature class. Each disease is represented by

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Geodatabase table. Relationships classes in the Geodatabase manage the associations between objects in one class (feature class or table) and objects in another [5]. Objects at either end of the relationship can be features with geometry or records in a table.

3.3 Editing Layers using ArcMap.

We use editing tools of ArcMap 10 to edit *"Veterinary Units*" layer on the map see Fig (5.a). All diseases layers joined with *"Veterinary Units*" layer see Fig (5.b).

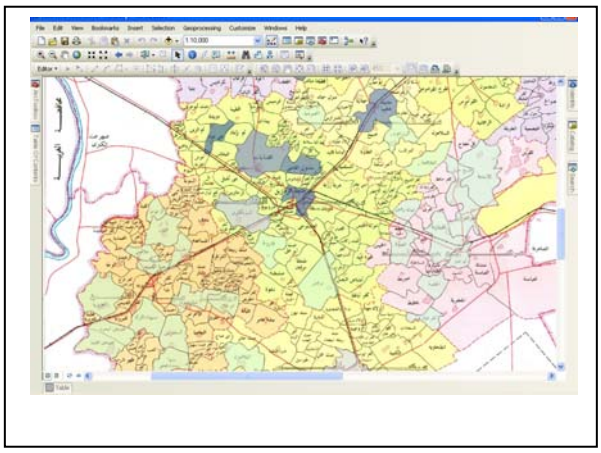


Fig 5. a: El Sharkeya Governorate Map with Veterinary Units

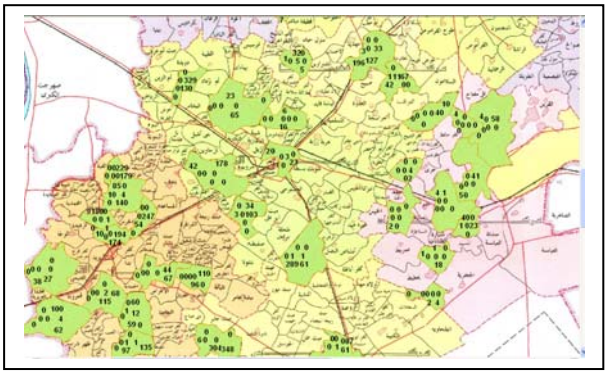


Fig 5. b: El Sharkeya Governorate Map with Diseases Count in Each Veterinary Unit

3.4 Drive New Data Layers (Raster)

Prepare and unify layers format to be Raster data. There are several ways to think about converting raster data in ArcGIS. You may want to convert non raster data into raster data or vice versa, such as converting a polygon into a raster. "*Diseases*", "*Economical*", "*Soil Pollution"* and "*Climate*" layers are converted from Polygon to Raster.

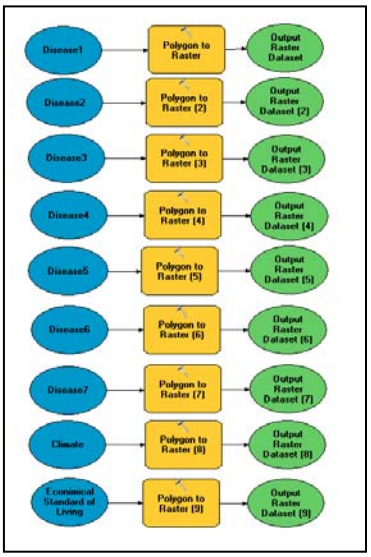


Fig 6. Convert Polygon to Raster

3.5 Reclassify Data

Reclassify data to values range from 1 to 9, all data reclassified to give weights. 9 is the most suitable value for animal production and 1 is the least.

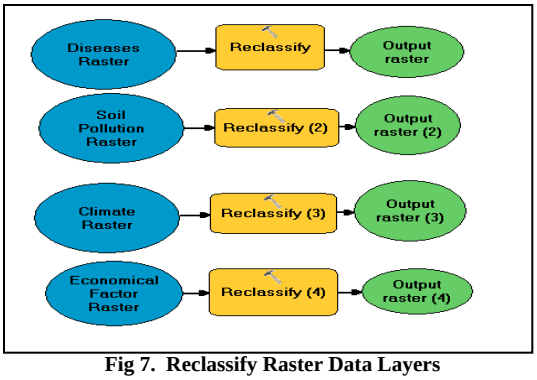


Fig 7. Reclassify Raster Data Layers

3.6 Weight and Combine Layers

Overlays several raster using a common measurement scale and weights each according to its importance. Seven diseases layers weighted using weighted overlay see Fig

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

(8). Output layer of weighted diseases weighted with "*Economical*", "*Soil Pollution"* and "*Climate*" layers see Fig (9).

Overlays several raster using a common measurement scale and weights each according to its importance. Seven diseases layers weighted using weighted overlay see Fig (8). Output layer of weighted diseases weighted with "*Economical*", "*Soil Pollution"* and "*Climate*" layers see Fig (9).

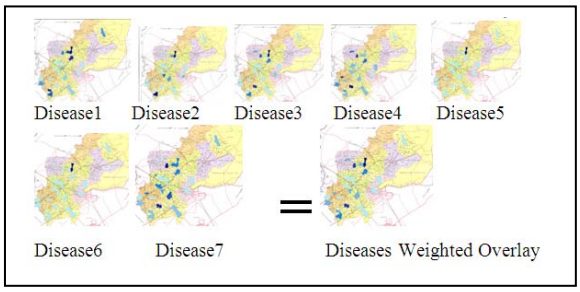


Fig 8.a: Weighted Overlay Diseases

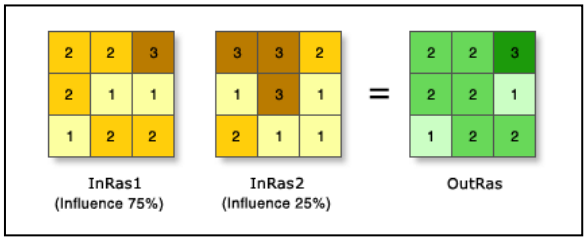


Fig 8.b: Weighted Overlay Influence

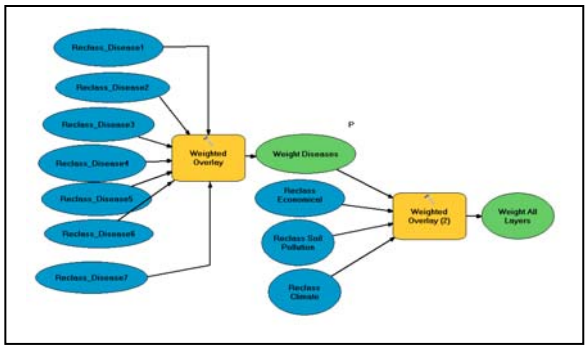


Fig 9. Weighted Overlay for All Factors with Different Influence

- All input raster must be integer. A floating-point raster must first be converted to an integer raster before it can be used in Weighted Overlay.
- Each value class in an input raster is assigned a new value based on an evaluation scale. These new values are reclassifications of the original input raster values. A restricted value is used for areas you want to exclude from the analysis.
- Each input raster is weighted according to its importance or its percent influence. The weight is a relative percentage, and the sum of the percent influence weights must equal 100.
- Changing the evaluation scales or the percentage influences can change the results of the weighted overlay analysis.

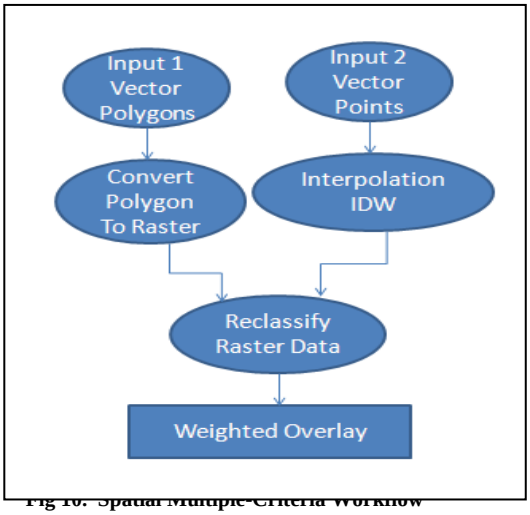


Fig 10: Spatial Multiple-Criteria Workflow

4. Results

Weighted overlay spatial analysis of diseases results indicate the following see Fig (11):

- Worst veterinary unit in EL Sharkeya governorate is Kofor Negm unit. This unit contains the highest diseases frequency.
- Best veterinary units are El Qeniat, El Zenkalon, Belbess, El Azezia and El Ketawia.

There are different units in middle diseases frequency such as El Sanafen, Mashtol El Soq and El Balashon.

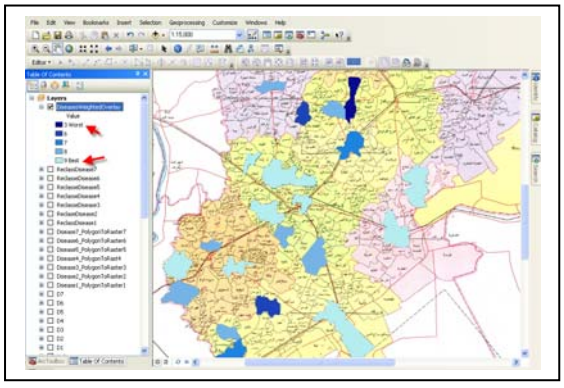


Fig 11. Diseases Weighted Overlay Results

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Diseases are an important factor in animal production. For instance, we supposed the following:

- The weighted diseases output layer influence is 50%.
- Economical factor influence represents 18%.
- Soil Pollution and Climate factors influence represent 16% for each factor.

Influence of each factor can be changed according its importance. The result of weighted overlay for factors affects animal production in Egypt represented in Fig (12). The value 3 represents the worst places for animal production in EL Sharkeya governorate and the value 8 represents the best places as in Fig (12).

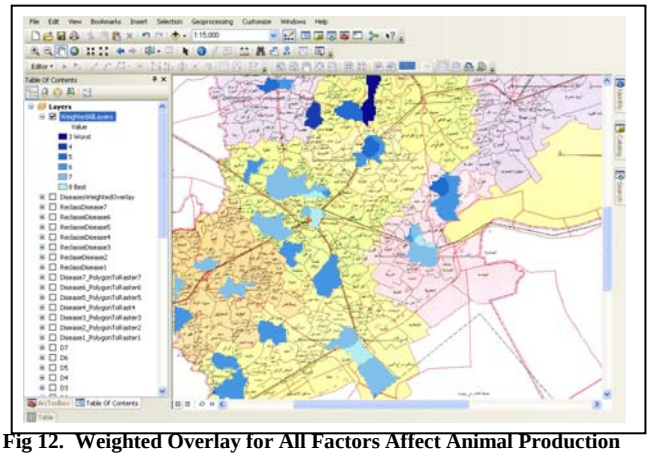


Fig 12. Weighted Overlay for All Factors Affect Animal Production in Egypt.

5. Conclusion

This paper presents an approach for helping policy/decision makers to improve animal production in Egypt. We visualize and analyze different factors such as "*Diseases*", "*Climate*", "*Soil Pollution*", "*Veterinary care*" and "*Economical factors*" which affect the animal production in Egypt. The paper takes in consideration influence of each factor because importance and influence of each factor differs according policy/decision makers point of view. In this research we aim to present the best way to visualize animal diseases and find the best and worst places in EL Sharkeya Governorate for animal production. We use weighted overlay spatial analysis to indicate that the worst veterinary unit in EL Sharkeya Governorate is Kofor Negm unit. This unit contains the highest diseases frequency and with weight equal 3, where as the best veterinary units are El Qeniat, El Zenkalon, Belbess, El Azezia and El Ketawia. The later units contain the lowest diseases frequency and with weight equal to 9. On the other hand we try to present other factors and study their influence on the decision making. For instance, we supposed the following:

- The weighted diseases output layer influence is 50%.
- Economical factor influence represents 18%.
- Soil Pollution and Climate factors influence represent 16% for each factor.

Anyway the influence of each factor can be changed according its importance at any time. The result of the weighted overlay for factors that affects animal production in Egypt is represented in Fig (12). As shown in this figure the value 3 represents the worst places for animal production in EL Sharkeya governorate and the value 8 represents the best places.

Acknowledgment

The authors wish to acknowledge the Central Laboratory for Agriculture Expert Systems (CLAES) in Egypt and ESRI Support Center.

References

[1] S. Gamal and H.Moussa, "Food Security in Egypt Under Economic Liberalization Policies and WTO Agreement", International Conference Agricultural policy reform and the WTO: where are we heading? Italy, 2007.

[2] El Fangary, L.M.; , "Mining Data of Buffalo and Cow Production in Egypt," *Frontier of Computer Science and Technology, 2009. FCST '09. Fourth International Conference on* , vol., no., pp.382-387, 17-19 Dec. 2009 doi:10.1109/FCST.2009.27
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5392891&isnumber=5392815.

[3] Omran, A.; Khorshid, M.; Saleh, M.; , "Intelligent decision support system for the Egyptian food security," *Intelligent Systems Design and Applications (ISDA), 2010 10th International Conference on* , vol., no., pp.557-562, Nov. 29 2010-Dec. 1 2010
doi: 10.1109/ISDA.2010.5687207
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5687207&isnumber=5687016.

[4] Rivest, S., Bédard, Y., Proulx, M.-J., Nadeau, M., Hubert, F., & Pastor, J. (2005). "SOLAP technology: Merging business intelligence with geospatial technology for interactive spatio-temporal exploration and analysis of data". ISPRS Journal of Photogrammetry and Remote Sensing, 60(1), 17-33. doi:10.1016/j.isprsjprs.2005.10.002

[5] Ahsan Abdullah "Analysis of mealybug incidence on the cotton crop using ADSS-OLAP (Online Analytical Processing) tool", Computers and Electronics in Agriculture,2009.

[6] P.J. Densham. "Spatial decision support systems". In D.J. Maguitre, M.F. Goodchild, and D. Rhind, editors, Geographical Information Systems:Principles and Applications. Longman, London, 1991.

[7] Maktav, D.; Jurgens, C.; Siegmund, A.; Sunar, F.; Esbah, H.; Kalkan, K.; Uysal, C.; Mercan, O.Y.; Akar, I.; Thunig, H.; Wolf, N.; , "Multi-criteria spatial decision support system for valuation of open spaces for urban planning," *Recent Advances in Space Technologies (RAST), 2011 5th International Conference on* , vol., no., pp.160-163, 9-11 June 2011
doi: 10.1109/RAST.2011.5966812
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5966812&isnumber=5966798.

[8] Yoon K, Hwang C, "Multiple attribute decision making – An introduction", SAGE Publications, Inc., Thousand Oaks, 1995.

Hesham A. Hassan is an Egyptian researcher born in Cairo in 1953. Hesham's educational background is as follows: B.Sc in Agriculture, Cairo University, Egypt in 1975. Postgraduate diploma in computer science, from ISSR, Cairo University, Egypt in 1984. M.Sc in computer science, from ISSR, Cairo university, Egypt, in 1989. Ph.D in computer science from ISSR, Cairo University (dual supervision Sweden/Egypt) in 1995. He is now a PROFESSOR and HEAD of computer science department at the faculty of computers and Information, Cairo University. He is also IT Consultant at Central Laboratory of Agricultural Expert System, National Agricultural Research Center. He has published over than 51 research papers in international journals, and conference proceedings. He has served member of steering committees and program committees of several national conferences. Hesham has supervised over 27 PhD and M. Sc theses. Prof. Hesham interests are Knowledge modeling, sharing and reuse, intelligent information retrieval, Intelligent Tutoring systems, Software Engineering. Cloud Computing and Service Oriented Architecture (SOA).

Hazem M. El-Bakry (Mansoura, EGYPT 20-9-1970) received B.Sc. degree in Electronics Engineering, and M.Sc. in Electrical Communication Engineering from the Faculty of Engineering, Mansoura University – Egypt, in 1992 and 1995 respectively. Dr. El-Bakry received Ph. D degree from University of Aizu - Japan in 2007. Currently, he is assistant professor at the Faculty of Computer Science and Information Systems – Mansoura University – Egypt. His research interests include neural networks, pattern recognition, image processing, biometrics, cooperative intelligent systems and electronic circuits. In these areas, he has published many papers in major international journals and refereed international conferences. According to academic measurements, now the total number of citations for his publications is 502. The H-index of his publications is 12 and G-index is 19. Dr. El-Bakry has the United States Patent No. 20060098887, 2006. Furthermore, he is associate editor for journal of computer science and network security (IJCSNS) and journal of convergence in information technology (JCIT). In addition, is a referee for IEEE Transactions on Signal Processing, Journal of Applied Soft Computing, the International Journal of Machine Graphics & Vision, the International Journal of Computer Science and Network Security, Enformatika Journals, WSEAS Journals and many different international conferences organized by IEEE. Moreover, he has been awarded the Japanese Computer & Communication prize in April 2006 and the best paper prize in two conferences cited by ACM. He has also been awarded Mansoura university prize for scientific publication in 2010 and 2011. Dr. El-Bakry has been selected in who Asia 2006 and BIC 100 educators in Africa 2008.

Hamada Gaber is an Egyptian researcher born in Cairo in 1985. He received the B.Sc degree in Computer and Information Sciences in 2006 from Assuit University, Egypt. He is currently a Master degree researcher in Mansoura University, Egypt.

The Agents scrutiny at Protocol Stack in NIDS

[1]Mr.M.Shiva Kumar, [2]Dr.K.Krishnamoorthy

[1]Research Scholar/Dept. of CSE/Karpagam University/Coimbatore/T.N,
[2]Professor & Head/Dept. of CSE/ Kuppam Engineering College/Kuppam/A.P.
email : shivasparadise@gmail.com

Abstract

The Research on the betterment of IDS and IPS is an avalanche process wherein each footstep paves way for new research work. In this regard This paper is a survey sheet on my research with respect to the implementation of Agents in the NIDS, first the paper depicts the OSI, later the impact of NIDS and the implementation of Agents in NIDS and it give a overview of the role of Agents in Basic Security Model and OSI reference and TCP/IP Model

Keywords : IDS,IPS,NIDS,TCP,IP,OSI.

1. An Overview of the Open Systems Interconnection Model

A NIDS is placed on a network to analyze traffic in search of unwanted or malicious events. Network traffic is built on various layers; each layer delivers data from one point to another.

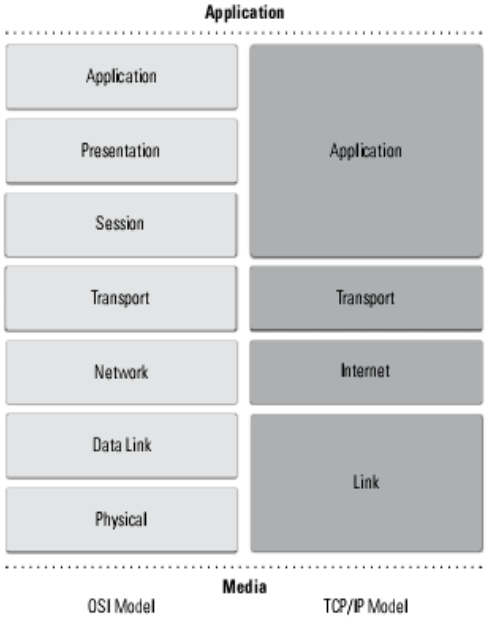


Figure 1. OSI and TCP/IP Model

The OSI model and transmission control protocol (TCP)/IP model show how each layer stacks up. (See Figure 1.) Within the TCP/IP model, the lowest link layer controls how data flows on the wire, such as controlling voltages and the physical addresses of hardware, like mandatory access control (MAC) addresses. The Internet layer controls address routing and contains the IP stack. The transport layer controls data flow and checks data integrity. It includes the TCP and user datagram protocol (UDP). Lastly, the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

most complicated but most familiar level is the application layer, which contains the traffic used by programs. Application layer traffic includes the Web (hypertext transfer protocol [*HTTP]),* file transfer protocol *(FTP),* email, *etc*. Most NIDSs detect unwanted traffic at each layer, but concentrate mostly on the application layer.

2. Component Types

Two main component types comprise a NIDS: appliance and software only. A NIDS appliance is a piece of dedicated hardware: its only function is to be an IDS. The operating system (OS), software, and the network interface cards (NIC) are included in the appliance. The second component type, software only, contains all the IDS software and sometimes the OS; however, the user provides the hardware. Software-only NIDSs are often less expensive than appliance-based NIDS because they do not provide the hardware; however, more configuration is required, and hardware compatibility issues may arise.

With an IDS, the "system" component is vital to efficiency. Often a NIDS is not comprised of one device but of several physically separated components. Even in a less complicated NIDS, all components may be present but may be contained in one device.but more specifically, the physical components usually include the sensor, management sever, database server, and console—

- **Sensor**—The sensor or agent is the NIDS component that sees network traffic and can make decisions regarding whether the traffic is malicious. Multiple sensors are usually placed at specific points around a network, and the location of the sensors is important. Connections to the network could be at firewalls, switches, routers, or other places at which the network divides.
- **Management server**—As the analyzer, a management server is a central location for all sensors to send their results. Management servers often connect to sensors *via* a management network; for security reasons, they often separate from the remainder of the network. The management server will make decisions based on what the sensor reports. It can also correlate information from several sensors and make decisions based on specific traffic in different locations on the network.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- **Database server**—Database servers are the storage components of the NIDS. From these servers, events from sensors and correlated data from management servers can be logged. Databases are used because of their large storage space and performance qualities.

- **Console**—As the user interface of the NIDS, the console is the portion of the NIDS at which the administrator can log into and configure the NIDS or to monitor its status. The console can be installed as either a local program on the administrator's computer or a secure Web application portal. Traffic between the components must be secure and should travel between each component unchanged and unviewed. Intercepted traffic could allow a hacker to change the way in which a network views an intrusion.

2.1NIDS Sensor Placement

Because a sensor is the portion of the NIDS that views network traffic, its placement is important for detecting proper traffic. Figure 2 offers an example of how to place a NIDS sensor and other components. There are several ways to connect a NIDS sensor to the network—

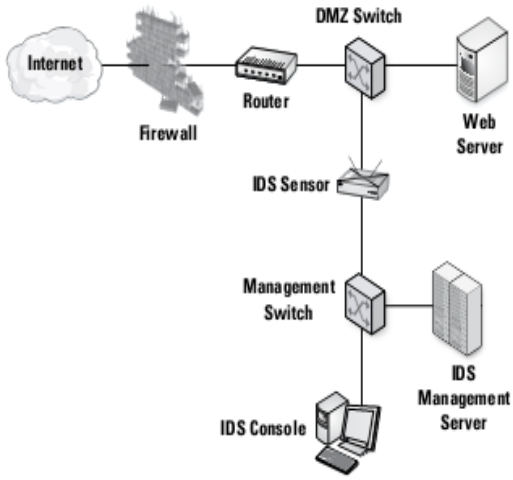


Figure 2. NIDS PLACEMENT

- **Inline**—An inline NIDS sensor is placed between two network devices, such as a router and a firewall. This means that all traffic between the two devices must travel through the sensor, guaranteeing that the sensor can analyze the traffic. An inline sensor of an IDS can be used to disallow traffic through the sensor that has been deemed malicious. Inline sensors are often placed between the secure side of the firewall and the remainder of the internal network so that it has less traffic to analyze.

- **Passive**—A passive sensor analyzes traffic that has been copied from the network versus traffic that passes through it. The copied traffic can come from numerous places—

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- **Spanning port**—Switches often allow all traffic on the switch to be copied to one port, called a spanning port. During times of low network load, this is an easy way to view all traffic on a switch; however, as the load increases, the switch may not be able to copy all traffic. Also, if the switch deems the traffic malformed, it may not copy the traffic at all; the malformed traffic that may be the type the NIDS sensor must analyze.
- **Network tap**—A network tap copies traffic at the physical layer. Network taps are commonly used in fiber-optic cables in which the network tap is inline and copies the signal without lowering the amount of light to an unusable level. Because network taps connect directly to the media, problems with a network tap can disable an entire connection.

2.2 Types of Events

A NIDS can detect many types of events, from benign to malicious. Reconnaissance events alone are not dangerous, but can lead to dangerous attacks. Reconnaissance events can originate at the TCP layer, such as a port scan. Running services have open ports to allow legitimate connections. During a port scan, an attacker tries to open connections on every port of a server to determine which services are running. Reconnaissance attacks also include opening connections of known applications, such as Web servers, to gather information about the server's OS and version. NIDS can also detect attacks at the network, transport, or application layers. These attacks include malicious code that could be used for denial of service (DoS) attacks and for theft of information. Lastly, NIDS can be used to detected less dangerous but nonetheless unwanted traffic, such as unexpected services (*i.e.,* backdoors) and policy violations.

3. Prevention

Although the detection portion of an IDS is the most complicated, the IDS goal is to make the network more secure, and the prevention portion of the IDS must accomplish that effort. After malicious or unwanted traffic is identified, using prevention techniques can stop it. When an IDS is placed in an inline configuration, all traffic must travel through an IDS sensor. When traffic is determined to be unwanted, the IDS does not forward the traffic to the remainder of the network. To be effective, however, this effort requires that all traffic pass through the sensor. When an IDS is not configured in an inline configuration, it

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

must end the malicious session by sending a reset packet to the network. Sometimes the attack can happen before the IDS can reset the connection. In addition, the action of ending connections works only on TCP, not on UDP or internet control message protocol (ICMP) connections. A more sophisticated approach to IPS is to reconfigure network devices (*e.g.*, firewalls, switches, and routers) to react to the traffic. Virtual local area networks (VLAN) can be configured to quarantine traffic and limit its connections to other resources.

4. Related work - Application of Agents to NIDS

As per the ongoing Research , the concept of Agent as seen in SMTP, sounds better in case of NIDS, either for Prevention or Detection, here I propose the application of Agents as shown in figure 3. (Agents Role in Basic Security Model)

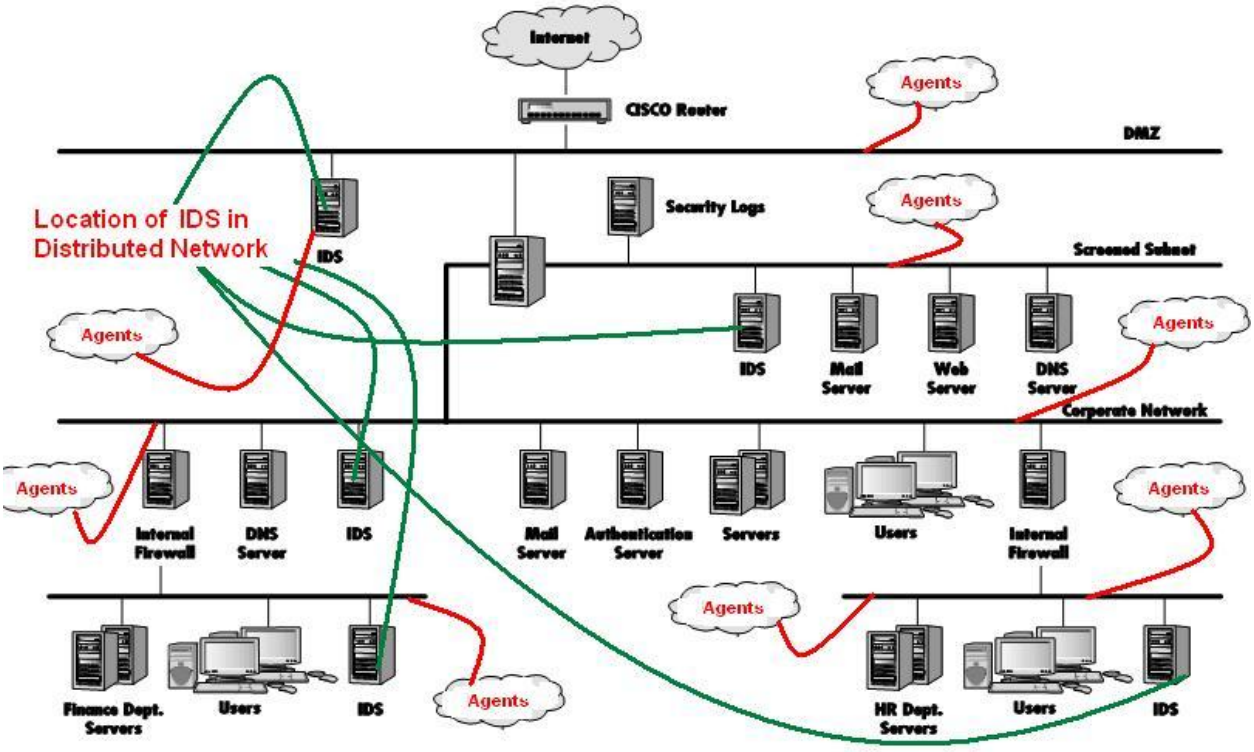


Figure 3. Basic Security Model

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

As in figure 3. We can find the IDS located in all the layers of the security channel, wherein it sounds or creates hazards in distributed networks paving way for the intruders.

Accordingly the implementation of Mobile Agents in the network monitors the network, here the agents work based on the NIDS that supports Anomaly Intrusion Detection Procedure, thereby the multiplicity of the IDS servers can be reduced.

Further the figure 4 depicts the impact of agents in OSI and TCP/IP Model

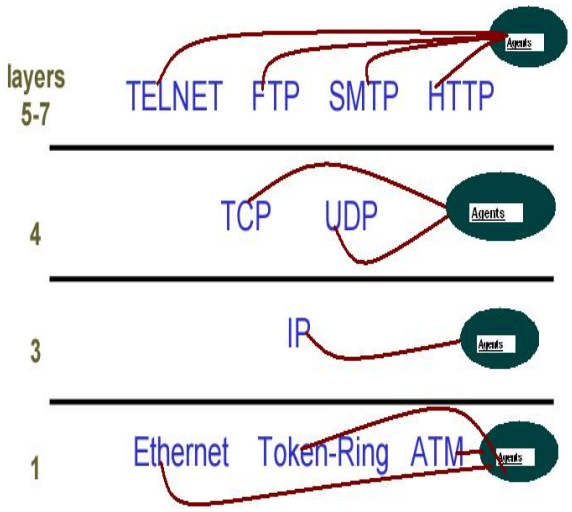


Figure 4. OSI Reference Model and TCP/IP with Agents.

The Role of Agents as depicted in the figure clearly shows the performance of the NIDS work in all the layers at the protocol stack level.

Since NIDS mainly concentrates on the Application layer ,here my research clearly shows the merits of IDs when implemented at each layer. Wherein individual agents with AIDS & NIDS work autonomously at each layer for each protocol.

In case of TCP, if Three way handshaking is to be considered, there is a possibility of attack during the time interval period in receiving the SYN from the receiver, with the invent of agents in the TCP/IP Protocol suite, it overcomes the misuse of services.

Conclusion

In this Paper I have just proposed a novel approach for implementing the Agents at the Protocol Stack, further enhancing the performance of NIDS, more importance to be given to the authentication features by implementing the Agents at KERBEROS.

Biography



Mr.M.ShivaKumar, Research Scholar, Department of CSE, Karpagam Universty, Coimbatore, T.N, India. having published papers in various conferences (National & international)
With good academic line of experience, Presently working has Associate Professor & head , in the Department of CSE, PNS INSTITUTE OF TECHNOLOGY, Nelamangala,Bangalore,Karnatka, india.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500



Dr.K.KrishnaMoorthy, Professor, Department of CSE, Sona College of Technology, Salem, T.N, India, has vast Experience and published papers in various conferences (National & international)

References

[1] M. Eid, "A New Mobile Agent-Based Intrusion detection System Using distributed Sensors", In proceeding of FEASC, 2004.

[2] G. Hulmer, J. S.K. Wong, V. Honavar, L. Miller, Y. Wang, "Lightweight Agents for Intrusion Detection", Journal of Systems and Software 67 (03), pages 109-122, 2003.

[3] M. Benattou and K. Tamine, "Mobile Agents Community For Distributed Intrusion Detection System", accepted for publication in proceeding of International conference on Computing, Communication and Control Technologies, Austin, USA, July 2005.

[3] B. Mukherjee, L.Todd Heberlein, and Karl N. Levitt. Network Intrusion Detection. IEEE Network,May/June 1994

[4] R. Janakiraman, M. Waldvogel, and Qi Zhang. Indra: a peer-to-peer approach to network intrusion detection and prevention. Twelfth IEEE International Workshops, Jun 9-11, 2003

[5] Fayyad, U., Piatetsky-Shapiro, G., and Smyth, P. 1996. The KDD process of extracting useful knowledge from volumes of data. Commun. ACM 39, 11, 27-34

[6] Zhou, L. and Haas Z.,"Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, November/December 1999.

[7] S. Puttini, J-M. Percher, L. Mé, O. Camp, R. de Sousa Jr., C. J. Barenco Abbas, L. J. Garcia Villalba. A Modular Architecture for Distributed IDS in MANET. In Proceedings of the 2003 International Conference on Computational Science and Its Applications (ICCSA). Springer Verlag, LNCS 2668, May 2003

[8] Kong, J., Luo, H., Xu, K., Gu, D., Gerla, M., and Lu, S.,"Adaptive Security for Multi-layer Ad-hoc Networks," Special Issue of Wireless Communication and Mobile Computing, 2002.

[9] Wenke Lee, Salvatore J. Stolfo. A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security (TISSEC) Vol. 3, Issue 4 Nov 2000

[10]GUIDE TO INTRUSION DETECTION AND PREVENTION (IDP) SYSTEMS (DRAFT) - Recommendations of the National Institute of Standards and Technology - Karen Kent & Peter Mell

[11]NIST SP 800-92 (DRAFT), Guide to Computer Security Log Management, which is available at http://csrc.nist.gov/publications/nistpubs/.

[12]The Cryptographic Module Validation Program (CMVP) at NIST coordinates FIPS testing; the CMVP Web site is located at http://csrc.nist.gov/cryptval/.

[13]http://csrc.nist.gov/cryptval/des.htm for information on FIPS-approved symmetric key algorithms.

[14] N Thanthry, M.S. Ali, and R Pendse, "Security, Internet Connectivity and Aircraft Data Networks," IEEE Aerospace and Electronic System Magazine, November 2006

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Analytical study to Measure Employee satisfaction in Jordan e-government applications

E- Diwan Project- in prime minister office in Jordan

Bashar H. Sarayreh
Management Information Systems Department
Information Technology College
Arab Academy for Banking and Financial Sciences
Amman Jordan
Bsarayreh@gmail.com

Mohamad M. Al-Laham
Al-Balqa Applied University
Amman University College
MIS Department
Amman, Jordan
Laham1st@yahoo.com

***Abstract*— there is a tremendous need by governments around the world to take advantage of the information revolution particularly the field of Enterprise resource planning and E-government in ordered to attain the optimum method of recourses investment. Traditionally e-government development is organized in to different phases (requirements, analysis, design, implementation, testing and maintenance). To assess whether e-government models we implementing meets all different user requirements in order to increase user performance. E-government model with a large diversity of users suffer from failures to satisfy heterogeneous requirements. A solution for this damaging situation is by deeply and in detail studying and analyzing user satisfaction factors. The future development try to avoid such unsatisfied factors which disturb user and minimized there performance. E-government is considered as hot topic tackled by many researchers as it is considered as future fact especially for the developing countries. This research introduces a case study: Analytical study to Measure Employee satisfaction in Jordan e-government applications: E- Diwan Project- in prime minister office in Jordan.**

Keywords: e-government, Satisfaction, E-Diwan[i], ERP

I. INTRODUCTION

Amongst the many tools being developed to fight against corruption, lately there has been much focus on e-government using Information and Communication Technology (ICT) to open up government processes and enable greater public access to information. Usage of the term e-government is of recent origin and there is no commonly accepted definition [1]. E-Government is understood as the use of emerging ICTs like Internet, World Wide Web and mobile phones to deliver information and services to citizens and businesses. It can also include publication of information about government services on a web site, for example so that citizens can download application forms for a variety of services. It can also involve the actual delivery of services, such as filing a tax return, renewing a license, etc. and moreover sophisticated applications include processing on-line payments.

In developed countries, these services are offered in a self-service mode through internet portals, which are a single point of interaction for the citizen to receive services from a large number of departments. In developing countries, on-line services counters may operate in a department offering services related only to that department. In some countries, citizen service centers have been created at convenient locations where citizens can access on-line services of several departments. These counters are operated by department/private operators, and the citizens do not directly interact with computer screens. Collection of payments is often then handled through conventional means. In addition to such service centers, citizens may also be able to access service delivery portals.

The benefits to citizens and businesses from on-line delivery of services include convenience (location and time) and shorter waiting periods. In addition, E-Government systems may lead to greater transparency, resulting in reduced administrative corruption [43].

II. E-GOVERNMENT IN JORDAN

E-Government is a National Program initiated by his Majesty King Abdullah II. The purpose of this program is to enhance the performance of government in terms of service provision, efficiency, accuracy, time and cost effectiveness, transparency, high level of customer satisfaction, cross-Governmental integration, and much more of elements related to the style the Government of Jordan works and perception of others to the Government [4].

The e-Government Program will support government transformation, using ICT tools to achieve the ultimate National goals. This transformation process requires a focal point of contact to coordinate the efforts between Government entities and support them with best practices and subject matter expert. Therefore, the Ministry of Information and Communications Technology (MoICT) was assigned to take the lead in implementing the e-Government Program, facilitating and providing support whenever needed to Government entities. For this purpose, MoICT has established a Program Management Office (PMO) and hired subject matter experts in areas of project management, change management, technical management and support services, risk management, quality management and other competencies.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The role of e-Government program is to plan, facilitate, manage and supervise the implementation of the following: Business Process Re-engineering (BPR) towards better and more efficient processes, human performance development (including knowledge transfer and training), organizations review and re-structuring to have more efficiency. Additionally, the e-Government deploys best practices and latest technologies to enable Government stakeholders implement new processes and create a knowledge-based community [3].

The e-Government vision is to be a major contributor to Jordan's economic and social development by providing access to Government e-Services and information for everyone in the Kingdom irrespective of location, economic status, ICT ability and education .The mission of e-Government is to manage the transformation of the government towards a more "customer-centric" approach in the delivery of services by means of appropriate technology, knowledge management and skilled staff to implement e-Government initiatives and programs that are relevant and affordable to the citizens of Jordan. E-Government Program is a major contributor to the Government of Jordan's administrative reform [3].

III. E-GOVERNMENT SOLUTIONS IN JORDAN:

CNS (computer network systems group) has been selected as one of the five prime companies for the development of the E-Government in Jordan. In addition to that, we have been working with government ministries, agencies, and departments prior to being selected, and after being selected for the development of each of these agencies unique solutions. One of the projects we have worked on is the E-Diwan of the Prime Ministry of Jordan. The E-Diwan is an e-service at the Prime Ministry's website designed for allowing other ministries and government departments to browse their incoming mail online before receiving it through regular mail. The system is designed to allow certain users at GoJ ministries and departments to log onto a secure area of www.pm.gov.jo and retrieve their incoming mail from the archive system at the Prime Ministry. Prime Ministry officials on the other hand are able to check who logged on and retrieved their correspondence online

Prime Ministry website & online application (www.pm.gov.jo): CNS was responsible for the design and development of this website. It was done based on the e-government look and feel, which was chosen according to the first two fast-track projects finished in 2002. It has a facility that enables the visitor from viewing the latest decisions and news the PM has taken on a daily basis. The visitor can also trace back Jordanian governments since the establishment of The Hashemite Kingdom of Jordan. The website has a section that deals with e-government that is developed by CNS as well, and is called "E-Diwan".

IV. E-DIWAN

The "E-Diwan" is an e-service at the Prime Ministry's website designed for allowing other ministries and government departments to browse their incoming mail online before receiving it through regular mail. The system in its first phase is designed to allow certain users at GoJ ministries and departments to log onto a secure area of www.pm.gov.jo and retrieve their incoming mail from the archive system at the Prime Ministry. The officials on the other hand are able to check who logged on an retrieved their correspondence online. The technologies used for this system were ORACLE, ASP, Cold Fusion, Perl, and Docuware (ARCHIVING SYSTEM).

V. USER SATISFACTION:

User satisfaction has received considerable attention of researchers since the 1980s as an important proxy measure of information systems success [7],[8]Several models for measuring user satisfaction were developed, including the user information satisfaction instrument [22] and a 12- item EUCS instrument [12],[. In one of the early studies, Bailey and Pearson (1983) developed a tool for measuring and analyzing computer user satisfaction of 39 items [6]. This instrument included many factors ranging from information quality, systems performance, personal relationship with electronic data processing (EDP) staff and top management involvement. Limitations of the study involved small sample size (29 valid data) and difficulty of applying the questionnaire. Baroudi et al [7] adopted the instrument by Bailey and Pearson [7] and examined causal relations of user involvement on system usage and information satisfaction. They concluded that user involvement in the development of information systems enhances both system usage and User's satisfaction with the system.

Ives et al [22] developed a User Information Satisfaction (UIS) instrument to measure user's general satisfaction with the information provided by the data processing group of the organization. Limitations of the study included use of an instrument that was based on the data processing computing environment. The emphasis was on computing tasks that were carried out by the data processing group in an organization. The measuring scale was semantic differential rather than Likert-scale type scaling. Due to the limitations of this study, this instrument is not used as much as the EUCS instrument developed by Doll and Torkzadeh [14].

Doll and Torkzadeh developed a 12-item EUCS instrument by contrasting traditional data processing environment and end-user computing environment, which comprised of five components: content, accuracy, format, ease of use, and timeliness. Their instrument was regarded as comprehensive, because they reviewed previous work on user satisfaction in their search for a comprehensive list of items. They included measurement of ease of use and this was not included in earlier research.

VI. AIMS OF THE RESEARCH:

The aim of this research is try to evaluate user satisfaction through evaluating some user satisfaction factors in both systems' related and works' related attributes in e-government in Jordan. These attributes will be reveled and confirmed through survey on how much users are satisfied from e-government services (E-Dwain) in Jordan.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VII. THE RESEARCH PROBLEM:

The problem in this research is the one size fit all approach as well as the stereotyped image of what will satisfy user from the e-government project team toward building e-government model, which may not suite user depending on many factors [7],[22],[8] this could leads to a waste of money to invest in the traditional web building machines. Therefore, a more suitable approach in defining user requirements is needed.

Study questions:

What are the relationships between users' satisfaction and work related attributes?

Study hypothesis:

H1: There is a Positive direct Relationship between User satisfaction and utilizing E-Diwan system and work related attributes.
H1.1: There is a positive direct relationship between user satisfaction and users' Degree of training.
H1.2: There is a positive relationship between user satisfaction and users' Understanding of systems.
H1.3: There is a positive relationship between user satisfaction and the degree of top management involvement.
H1.4: There is a positive relationship between user satisfaction and users' Feeling of control.

Research methodology

Two approaches were highlighted by Alkhaldi [3] that research methodology can be consequent from. These approaches can be classified into two main approaches. These two categories are sometimes illustrated by different terms. The positivistic approach can sometimes be described as traditional, quantitative, or empiricist. While the phenomenological approach can be labeled as post-positivistic, subjective, or qualitative ,According to Alkhaldi [3] the positivistic approach is largely based on quantitative data. Explaining causality requires the establishment of relationships between variables and linking them to a certain theory. The benefits of positivistic approach are cost effective and speed in data collection, the ease of analysis, apposite for testing hypotheses and determining relations between variables and establishing the reliability and OF DATA.
The phenomenological approach or post positivistic, on the other hand, has emerged as a result of denunciation of the application of positivistic approach in social science.

STUDY POPULATION AND SAMPLE:

The study population is user for "E-Diwan" who uses the system in order to get information or to achieve different services. A purposeful sampling methodology will be adapted in order of the sample to will be representative and to reflect the study objectives.

Data collection and information resources:

The data and information will be gathered from two resources: the Primary resources: User satisfaction survey which will be designed to get the primary resources, and the secondary resources: through books and the scientific references concerned with the study subject.

Suggested statistical methods:

EQS 6.1 is an advance statistical tool which will be utilized in order to analyze collected data, and the following Statistical Methods Are Suggested: Cronpach Alpha For Reliability Test. Descriptive Analysis.Factor Analysis; Explanatory and Confirmatory Structural Equation Modeling.

Confirmatory Model Testing:

Work Related Attributes Test Model Degree of Training:
H1.1: There is a positive direct relationship between user satisfaction and users' Degree of training.
The review of the hypothesized model reveals that the t-value (t=4.2) of the completely standardized coefficient of training → WRA regression path is significant. The structural equation fit is as follows, The coefficient of determination R^2 of the training (regression path: training → WRA) = 0.14 shows that 14% of the total variance in WRA creation activities was accounted for by the training.

- Understanding of the System:

H1.2: There is a positive relationship between user satisfaction and users' Understanding of systems .
The review of the hypothesized model reveals that the t-value (t=9.3) of the completely standardized coefficient of Understanding → WRA regression path is significant. The structural equation fit is as follows, The coefficient of determination R^2 of the Understanding (regression path: Understanding → WRA) = 0.65 shows that 65% of the total variance in WRA creation activities was accounted for by the Understanding.

- Top Management Involvement:

H1.3: There is a positive relationship between user satisfaction and the degree of top management involvement
The review of the hypothesized model reveals that the t-value (t=4.8) of the completely standardized coefficient of

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Top management → WRA regression path is significant. The structural equation fit is as follows, The coefficient of determination R^2 of the Understanding (regression path: Understanding → WRA) = 0.17 shows that 17% of the total variance in WRA creation activities was accounted for by the Top management.

Feeling of Control:

H1.4: There is a positive relationship between user satisfaction and users' Feeling of control.

The review of the hypothesized model reveals that the t-value fixed of the completely standardized coefficient of Feeling of control → WRA regression path is significant. The structural equation fit is as follows,

The coefficient of determination R^2 of Feeling of control (regression path: Feeling of control → WRA) = 0.52 shows that 52 % of the total variance in WRA creation activities was accounted for by Feeling of control.

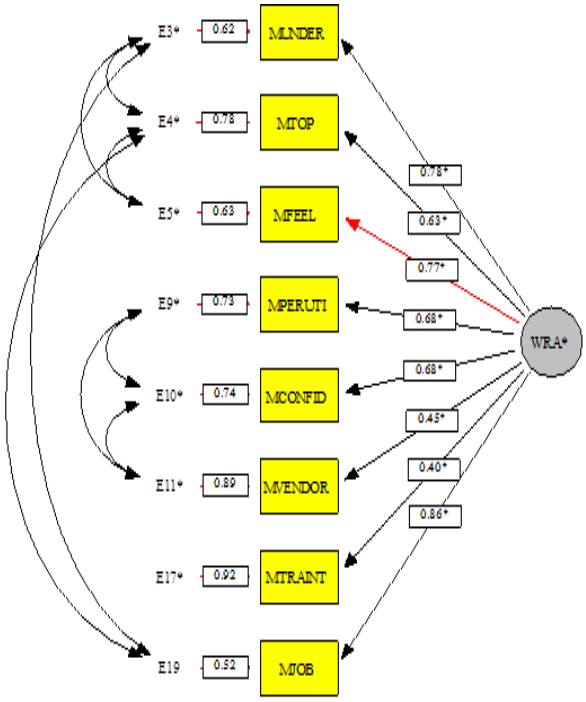


Figure X: EQS 6 wra_v8 Chi Sq.=22.40 P=0.05 CFI=0.99 RMSEA=0.07

VIII. Result and Recommendation

This resaerch began with the observation that measuring a success of information technology system which requires first, a new settlement of what make a IS a success and from what point of view the organization or the user satisfaction or both. This research has investigated major questions. 'What are the characteristics of a successful IS system?' 'How to measure user satisfaction in complex systems like e-government?' 'Why to measure user satisfaction as the main indicator and not organization satisfactions?' To answer these questions, the study utilizes, redefines and then expands [38];[39];[40];];[18].

Literature and the model which clearly highlight that "IS Success" which is a field containing much debate. A questionnaire survey was performed on the context of Jordan environment to increase the understanding of the factors effecting IT success mainly user satisfactions, to quantify the factors of interest and to test for their autonomous and shared effect and relationship to IS success in a complex system. The research utilized advanced multivariate statistical techniques (CFA and SEM enabled by EQS 6.1 software). This led to a number of compelling findings.

IX. Summary of the Main Findings

The overall results of the empirical investigation did support the general framework. Using confirmatory factor analysis, the user satisfaction hypotheses developed for this research was tested and the model were also verified. IT satisfaction factors seen by work (WRA) related factors were confirmed.

The results indicated that the phases of user satisfaction from complex systems. in the Degree of training test highlight that that there is dissatisfaction to the time spent on training hours and the overall there are a general satisfaction of the system depending on training. Also in the Understanding of system test, Confirmed that the degree of understanding there is general satisfaction. Moreover, the Top management involvement test shows that the degree of Top management involvement is less satisfying. Also the Feeling of control test clearly indicates that the degree of Feeling of control is satisfying that refers to less sufficient training and understanding the system. In the Job effect test it is indicated that the degree of Job effect is satisfying.

References

[1] CHRI 2003 Report OPEN SESAME: looking for the Right to Information in the Commonwealth, Commonwealth Human Rights Initiative, 2003. Subhash Bhatnagar

[2] Alloway, R.M., and Quillard, J.A. (2001) "User Managers' Systems Needs", MIS Quarterly, Vol. 91.

[3] http://www.moict.gov.jo/en-us/homepage/studiesandreports.aspx.

[4] Alkhaldi, Firas. An Integration of Information Technology, Culture of Knowledge Transfer and Innovative Work Environment in Support of Organizational Knowledge Creation Activities, Unpublished PhD Thesis, University of Huddersfield, 2003.

[5] Tadros, ibrahem . Al-shekh, Assem . Abdali, Rashed, (Success factors in Jordan e-government, IMB 2006, Australia.

[6] Baskerville, R. (1999). "Investigating Information Systems with Action Research". Communications of the AIS, Vol. 2, Article 19.

[7] Bailey, James E.; Pearson, Sammy. Development of a Tool for Measuring and Analyzing Computer User Satisfaction, Management Science, May 1983, Vol. 29 Issue 5, p530, 16p.

[8] Baroudi, J. J., Olson, M. H. and Ives, B. An Empirical Study of the Impact of User Involvement on System Usage and Information Satisfaction,. Communications of the ACM (29:3), March 1986, pp. 232-238.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[9] David H. Benson. A Field Study of End User Computing: Findings and Issues. MIS Quarterly, Vol. 7, No. 4 (Dec., 1983), pp. 35-45

[10] Francois Bergeron, Suzanne Rivard, Lyne de Serre. Investigating the Support Role of the Information Center. MIS Quarterly, Vol. 14, No. 3 (Sep., 1990), pp. 247-260.

[11] Chen, L., Soliman, K.S., Mao, E. and M.N. Frolick,. Measuring User Satisfaction with Data Warehouses: An Exploratory Study, Information & Management, Volume 37, Number 3, 1 April 2000 , pp. 103-110(8)

[12] Coopee, T. .The Internet Today,. InfoWorld (22:39), September 2000, pp. 52.

[13] 15. Doll, W. J. and Torkzadeh, G. .The Measurement of End-User Computing Satisfaction,. MIS Quarterly (12:2), June 1988, pp. 259-274. Quarterly (7:4), December 2002.

[14] Doll, William J.; Torkzadeh, Gholamreza The Measurement Of End-User Computing Satisfaction MIS Quarterly, Jun 1988, Vol. 12 Issue 2, p259, 16p...

[15] 18. William J. Doll, Weidong Xia, Gholamreza Torkzadeh . A Confirmatory Factor Analysis of the End-User Computing

[16] 19. Satisfaction Instrument. MIS Quarterly, Vol. 18, No. 4 (Dec., 1994), pp. 453-461

[17] 21. Fitzgerald, Edmond P. and Cater-Steel, Aileen (1995) Champagne training on a beer budget. Communications of the ACM, 38 (7). pp. 49-60.

[18] 23. Gallivan, M.J., "Examining Workgroup Influence on Technology Usage: A Community of Practice Perspective," in W. Nance (ed.) Proceedings of the 2000 ACM Special Interest Group on Computer Personnel Research, Chicago, IL., April 2000, 54-66.

[19] P. Weill, Univ. of Melbourne, Melbourne, Victoria Australia. M. H. Olson ... Volume 13 Issue 1, March 1989. Harris, D.P. (1999). An Investigation of the Factors Affecting Where Desktop Computer Users Go for Computer Support in an Academic Environment, Unpublished doctoral dissertation, Claremont Graduate School, USA.

[20] Henderson, J.C., and Treacy, M.E. (2003). "Managing End User Computing for Competitive Advantage," Sloan Management Review, winter 1986. pp. 3-14.

[21] Involvement on System Usage and Information Satisfaction,. Communications of the ACM (29:3), March 1986, .

[22] Ives, Blake; Olson, Margrethe H.; Baroudi, Jack J.The measurement of user information satisfaction , Communications of the ACM, Oct 1983, Vol. 26 Issue 10, p785, 9p

[23] Jupiter Media Metrix .U.S. Top 50 Web and Digital Media Properties., for December 2001

[24] http://www.jmm.com/xp/jmm/press/mediaMetrixTop50.xml

[25] Kerlinger, F. 1973. Foundations of Behavioral Research, McGraw-Hill, New York, 1973.

[26] Lamb, R. & Davidson, E. (2000). The New Computing Archipelago: Intranet Islands of Practice. In: Proceedings of the IFIPWG8.2 working conference on information technology and changes in organizational work, pp. 255-274.

[27] Larsen, T.J. (1993). "Middle Managers' Contribution to Implemented Information Technology Innovation". Journal of Management Information Systems, vol. 10, Issue 2, pp. 155-176.

[28] McHaney, R. and Cronan, T.P. .Computer Simulation Success: On the Use of the End-User Computing Satisfaction Instrument: A Comment,. Decision Sciences (29:2), March 1998, pp. 525-535.

[29] Xiao and Dasgupta/User Satisfaction with Web-Based Information Systems

[30] 2002 . Eighth Americas Conference on Information Systems 1155

[31] Mathieson, K. (1991). "Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior". Information Systems Research. Vol.2, Issue 3, pp. 173-191.

[32] McHaney, R. and Cronan, T.P.Toward an empirical understanding of computer simulation implementation success,. Information and Management (37), 2000, Issue 3 ,pp. 135-151.

[33] McHaney, R. Hightower, R. and White D. .EUCS test-retest reliability in representational model decision support systems. Information and Management (36), 1999, pp. 109-119.

[34] Olfman, L., Bostrom, R.P. and Sein, M.K. (2001). "Business Led Training: A Best Practice" Conference Proceedings, BITWorld 2001 Business Information Technology Management: Enabling Cultural Awareness, S. Kemal (Ed), June 2001, Cairo, Egypt.

[35] Subhash Bhatnagar, 2003 E-government and access to information

aleria Merino Dirani, Ecuador's first steps towards e-procurement

[36] Torkzadeh, G. and Doll, W. .Test-Retest Reliability of the End-User Computing Satisfaction Instrument., Decision Sciences (22:1), winter 1991, pp. 26-37.

[37] Garrity, E. J., & Sanders, G. L. (1998), Dimensions of information systems success, Information systems success measurement, pages 13-45.

[38] Gelderman, Maarten, 1998. "Usage of performance measurement and evaluation systems : the impact of evaluator characteristics," Serie Research Memoranda 0017, VU University Amsterdam, Faculty of Economics, Business Administration and Econometrics.

[39] Shirani, Aiken and Reithel's (1994) UIS model and from the American Customer Henson 1997; Shirani, Aiken and Reithel 1994; Suh, Kim and Lee 1994).

AUTHORS PROFILE

Bashar Sarayreh, PhD in Management Information Systems, He is Assistant Professor in Management Information Systems (MIS). His principal research interests include e business, quality and excellence model and information managements .

Mohamad Al-Laham, PhD in computer information Systems, He is Associate professor in Computer Information Systems (CIS). His principal research interests include human computer interaction, e-commerce and web development.

[i] The E-Diwan is an e-service at the Prime Ministry's website designed for allowing other ministries and government departments to browse their incoming mail online before receiving it through regular mail.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

BIO-THENTIC CARD: AUTHENTICATION CONCEPT FOR RFID CARD

Ikuesan Richard Adeyemi
Dept. computer science and information system
Universiti Teknologi, Malaysia
Johor Bahru, Malaysia

Norafida Bt, Ithnin
Dept. computer science and information system
Universiti Teknologi, Malaysia
Johor Bahru, Malaysia

Abstract
Radio frequency identification (RFID) is a technology that employs basic identifier of an object embedded in a chip, transmitted via radio wave, for identification. An RFID Card responds to query/interrogation irrespective of '*Who*' holds the Card; like a key to a door. Since an attacker can possess the card, access to such object can therefore be easily compromised. This security breach is classified as an unauthorized use of Card, and it forms the bedrock for RFID Card compromise especially in access control. As an on-card authentication mechanism, this research proposed a concept termed Bio-Thentic Card, which can be adopted to prevent this single point of failure of RFID Card. The Bio-Thentic Card was fabricated, tested and assessed in line with the known threats, and attacks; and it was observed to proffer substantive solution to unauthorized use of RFID Card vulnerability.

Key words: Vulnerability, unauthorized, mitigation, authentication, communication, access control system

I. INTRODUCTION

Radio frequency identification (RFID) technology is a technology that has gained wider adoption into the human everyday life since its first usage in identification friend or foe (IFF) during the II world war [1, 3]. RFID is characterized by its ubiquitous nature, flexibility, mobility and integratability, which has contributed to its adoption in places such as access control system, conveyor control system, banking notes, item identification e.t.c. While RFID pros have greatly improve other technology, its cons has also generated series of security and privacy challenges [2, 3, 6] some to the detriment of the system being integrated into [4, 5]. However, such challenges are not limited to only RFID systems, but peculiar to RFID systems, are attacks such as relay attack, cloning, clandestine tracking, unauthorized tag read, and unauthorized tag use [2, 6, 8] . Un-authorization of card use is a general challenge in access control system; hence, most systems would require a secondary control mechanism.

However, the integration of the RFID tag into access control Card otherwise known as RFID Card has further complicated the challenges in access control cards leading to greater trade-offs in security and privacy[3, 6,7, 8]. Access control RFID card do not provide on-card authentication system hence is openly vulnerable to attacks that breach the confidentiality of a secured system. RFID Card responds to interrogation from an RFID Reader irrespective of '*who*' holds the card, or whether the subject has the required privilege to do so. This lack of authorization priori to interrogation can be said to be the principal point of failure of the RFID Card. For instance, consider the situation where an unauthorized subject with malicious intent or the otherwise, gains access to a classified data through a stolen RFID Card and consequently jeopardize the confidentiality of the system under protection. It suffixes to note that, to the best of our knowledge, no known countermeasure addressed this single point of failure of the RFID Card.

However, mitigating this critical point of failure is not as trivial as it sounds. Faraday shield model in [1] is popular method (aluminum-foiled wallet for example) of shielding the RFID Card from unauthorized tag reading, thus enhancing the privacy protection of the RFID tag. The unauthorized tag use as applied to RFID Card is the main goal of this paper as analyzed in [31]. The remaining of this paper is organized as follows. Section II highlights the related research works on RFID tag with reference to its physical layer, discusses the principal point of failure of the RFID Card. Section III introduces the concept used in this study, detailed the design and result of this study. Section IV presents the analysis and the conclusion of this concept.

II. RELATED RESEARCH

RFID Card is a composition of antenna unit, memory unit, processing unit, and a tag, which communicates with an RFID Reader wirelessly using the near field coupling principle. Over the past decades researchers have worked extensively on the RFID system but interest on RFID on-card authentication system have received minimal attention. According to [4, 9], the physical layer of the RFID system is the perimeter defense line for security tightening in RFID system. RFID authentication protocols [10, 11, 12, 13, 14] are designed to mitigate communication attacks between the tag and the Reader. Similarly, various lightweight cryptographic protocols and techniques [15, 16, 17, 18, 19, 20,] have also been designed to combat security vulnerabilities in the RFID system. However, these authentication practices do not apply to the tag end of the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

physical layer of the RFID system. Additionally, techniques such as blocker tag [21], RFID guardian [22], RFID zapper [23], Faraday shield [30] and clipped tag [24] are mitigation to distance attacks, which does not necessarily translate affect RFID cards due to short range of communication. However, in [25], a framework for user's authentication procedure was modeled using fingerprint authentication through reader-system authentication process, a similar process to [26] which is adopts a two-factor authentication system based on combined fingerprint recognition and smart RF Card verification. They however failed to address the underlying problem of the on-Card authentication of the RFID card. In [27, 28] different categories of RFID card suitable for different security integration were designed but they lacked the core and essential component of card security: user authentication. [31] gives a detailed analysis of the challenges in RFID card with reference to its physical layer. Table 1 gives the summary of the various countermeasures proposed against the physical layer authentication vulnerabilities.

Table 1: Countermeasure to physical layer Authentication Challenges

Proposed Counter-Measure	**Authentication at Physical-Layer Vulnerabilities**								
	Unauthorized Card reading	Unauthorized Card	Tag cloning	Relay attack	Skimming	Spoofing	Unauthorized killing	Clandestine tracking	Physical layer Identification
Physical-Layer Identification technique	×	×	√	×	×	×	×	×	√
Faraday Cage	√	×	×	×	√	√	√	√	×
Authentication protocol	√	×	×	√	√	√	√	√	×
Clipped Tag	√	×	×	√	√	√	×	√	×
Anti-counterfeiting	√	×	√	√	√	√	√	×	×
Biometric authentication	×	×	×	×	×	×	×	×	√
Labeling	**ONLY create awareness for users**								
Controllable Tag	√	×	×	√	√	√	√	√	×

The physical layer identification technique [29] addresses cloning of tags, and proves that no two tags can have the same fingerprint. Furthermore, controllable tag[27] addressed the issue of unauthorized tag read, thus curbing one of the principal source of attacks on RFID tag. However, on-card authentication vulnerability, which is a major security challenge, have received little or no attention as shown in Table 1 Countermeasure such as clipped tag, and fingerprint biometric authentication [25] can be combined in a digitalized manner to curtail this challenge. In the next session we, present our concept of Bio-Thentic Card as a concept of On-Card authentication process, which is a combination of digitalized controllable clip tag and fingerprint authentication system.

III. ON-CARD AUTHENTICATION CONCEPT

The architecture of the RFID Card reveals that communication between the Card and the Reader is hinged on the interconnection between the antenna unit and the tag *inside of the* Card. The antenna (usually rectangular spiral) unit of the RFID card is the medium of interaction between the tag of the RFID Card and the RFID Reader. Hence, the connectivity, transmission range and power supply to the RFID tag is a function of the antenna unit. Suppose we represent the communication process as C_p which is the integration of the antenna unit joints (A_{uj}), and the RFID tag (R_t). For the sake of this paper, we represent every other parameter surrounding the RFID tag such as battery, memory unit, as RFID tag. We also assume that the antenna unit is the suitable antenna for RFID card. The communication process, $\boldsymbol{C}_p$ is given by *equation (i)*.

$$\boldsymbol{C}_p = \sum_{i=0}^{k} \left(\sum_{j=0}^{n} R_t \text{ x } A_{uj} \right) \qquad (1)$$

If $A_{uj} = 0$, then, the communication process $\boldsymbol{C_p}$ presented in equation (*i*) becomes:

$$\mathrm{C_p} = \sum_{i=0}^{k} \left(\sum_{j=0}^{n} R_t \text{ x } 0 \right) = 0 \qquad (2)$$

This illustrates that if the possible contact between the RFID tag and the antenna unit can be disconnected such that the total corresponding antenna unit connection is zero, then, the antenna communication process ($\boldsymbol{C_p}$) will be zero. With this criteria, we observed that the unauthorized use of card vulnerability in the RFID Card can be mitigated using the combination of digitally clippable tag-antenna-joint, and a biometric authentication system, preferably, fingerprint, as analyzed in [31]. Furthermore, we observed that a strategic placement of a digitally controllable hinge between the antenna and the tag in such as way that the antenna forms a shield around the tag, when totally disconnected from the tag, will prevent privacy disclosure, tracking and all radio wave related attacks. When this clippable joint is then strictly controlled by an authentic subject, the single point of failure of the RFID Card can thus be mitigated. We termed this concept Bio-Thentic Card (BTC), which is the integration of biometric component into the RFID tag

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

IV. RESEARCH METHOD

Our research aimed at conceptualizing an RFID Card (which we called BTC) which can mitigate the unauthorized Card use vulnerability. In order to achieve our aim, we designed our methodology into three distinct stages.

Stage1: this stage comprises the design, calibration, simulation and fabrication of the card antenna unit. In this stage, we analyzed thoroughly; the suitable positioning, and control of the clippable joint, such that the Card will respond to interrogation only through the contact from the clip joint.

Stage2: this stage involves the acquiring, authenticating, securing and storage of the biometric authentication process, fingerprint in this case. We carefully considered the choice of the fingerprint module to use in line with information security practices such as security of the fingerprint module (live fingerprint detection, and false error rate) and secure code development practice.

Stage3: this stage involves the integration of the various modules, and the control module. The result and testing process is detailed in the next session. The control unit integrates the biometric fingerprint and the fabricated antenna unit into a single module controlled by a microcontroller. Figure 1 gives a detailed description of the our designed methodology

The Output from the clip joint and the Faraday cage must be 'Yes' before stage1 can be passed to stage2 as shown in Figure 1. The communication between stages 1, 2 and 3 is illustrated in Figure 2. We designed a rectangular loop antenna consisting of stripped copper lines, with external dimension of 54x33mm, 0.5mm width, 7 turns, 1mm spacing and 0.035mm thickness using a computer simulation technology (CST) studio as shown in Figure 3 and 4. The design comprises a PCB made of FR4-lossy dielectric material with thickness of 1.6mm, dimension of 60x40mm, relative permeability of 1, and relative electric permittivity of 4.55.

We integrated the clipped joint as shown in Figure 3 through the fabrication process of the card antenna unit with a 13.56MHz RFID tag (see Figure 5). The digitalized controllable hinge was introduced through a miniature relay of 1A, 5V direct current, and internal coil resistance of 166ohms. Upon simulation, we arrived at an S-parameter value of -2.730712, which we considered as suitable for our experimental purpose as illustrated in Figure 4.

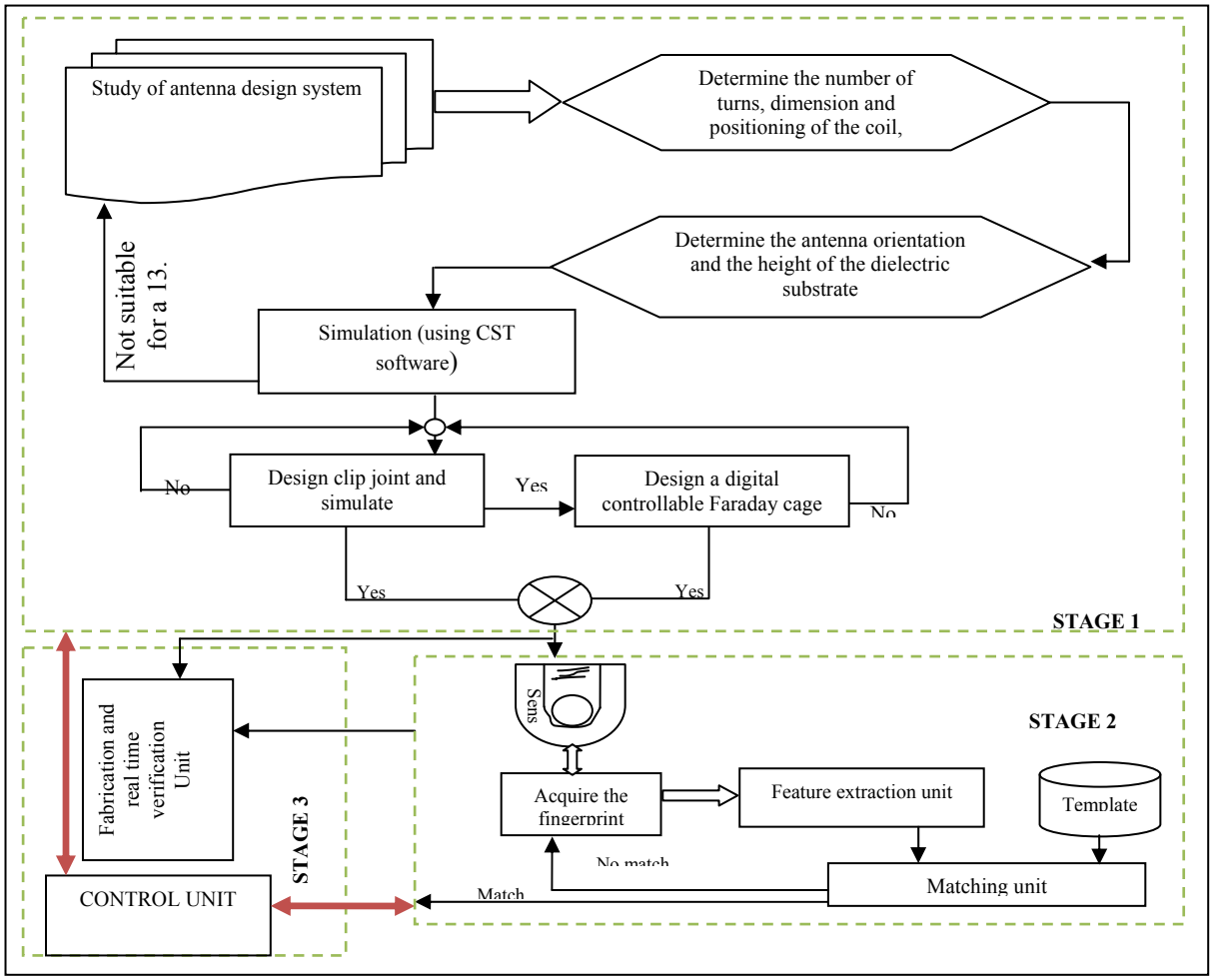


Figure 1: Design Flow Process

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

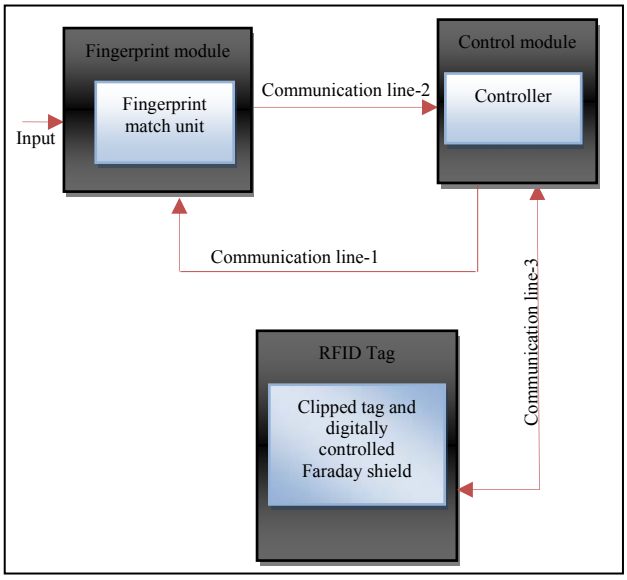


Figure 2: Communication process of the Bio-Thentic Card

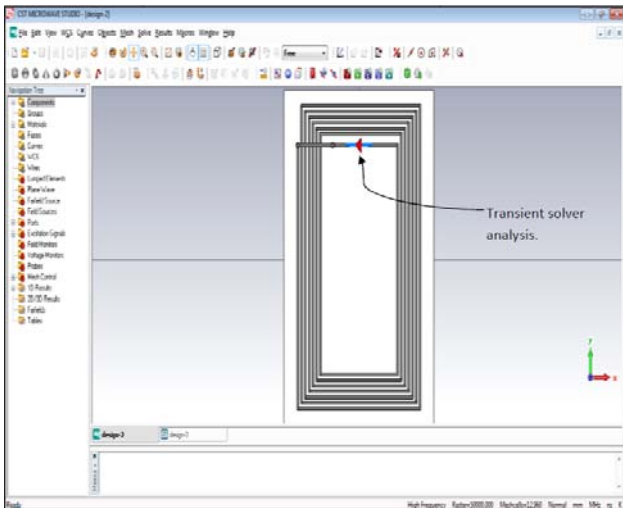


Figure 3: Antenna structure

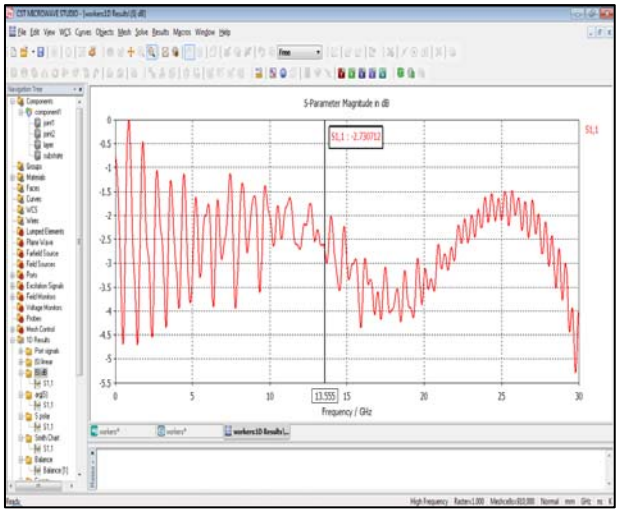


Figure 4: S-parameters as a function of frequency

V. BIO-THENTIC CARD (BTC)

A secured fingerprint module was adopted for the biometric authentication process. Moreover, it was designed as an on-card biometric match system. Two distinct fingerprints of the authentic user are required for the operation of the Card. Additionally; we stored other fingerprints templates for testing purpose, and tagged them with various identities. The communication process shown in Figure 4 depicts the link between the fingerprint module, and the antenna unit of the card controlled by the control unit. Visual description of the BTC is given in Figure 5.

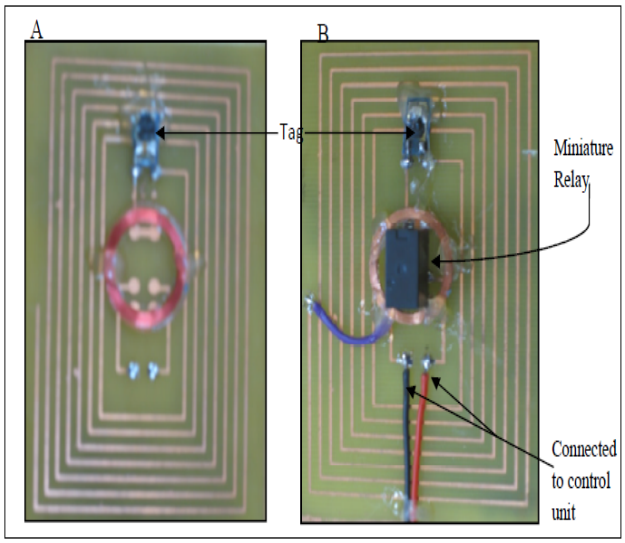


Figure 5: Fabricated Result of Antenna Unit

The control unit was designed using an Atmel AVR-Atmega-8515 microcontroller securely coded using assembly language and AVR studio 4. However, different light emitting diodes (LEDs) were used as indicator on the state of the Card at any given point in operation (see Table 2).

VI. DISCUSSION

We tested the concept following the procedure stated in Figure 6, and it responded as programmed, practically denying access to unauthorized user.
Furthermore, we subjected BTC to different degree of risk assessment, a process synonymous with fault testing in electronics, or penetration testing in networking environment. In order to evaluate this concept, we demonstrated the following risk assessment processes.
*Tag Manipulation***:** we placed the Card at various angles, proximities and direction to an RFID reader without due authorization from the authentic user. However, there was no interrogation. *Clip joint circumvention***:** We assumed that an attacker could gain access to the internal architecture of the Card (which is practically infeasible). We bridged the clip joint using connecting cables at first, and later using a 5v supply unit.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Table 2: Control Output Indication

Template label	Atmega-8515 Pin-out	Control Effect	Indication
A and B	PORTB, 6:4 PORTD 7	Miniature / Green-LED	Authorized user with access permission, access granted
C	PORTD, 6	Yellow-LED	Authorized user without access permission, access denied
D	PORTD, 5	Blue-LED	Unauthorized user, access denied
E	PORTD, 4	Red-LED	Unauthorized user, access denied (and further warning may be indicated

The former could not initiate the interrogation but the later attempted to trigger the switch trigger (a 5v relay in this case).

*Fingerprint manipulation***:** We forged an OHP film fingerprint of the residue print on the surface of the scanner. This forges film was then disguised as an authentic user. The evaluation process further proved the security potency of this concept. The fingerprint manipulation could not initiate interrogation due the secured practice exhibited in the requirement for authorization. However, we discovered that unauthorized tag use could be mitigated with this concept. In addition , a securely design process, and a more aligned fabrication process of the clip joint, such attack is practically infeasible or extremely expensive. Other forms of risk associated with the typical RFID Card can thus be successfully mitigated

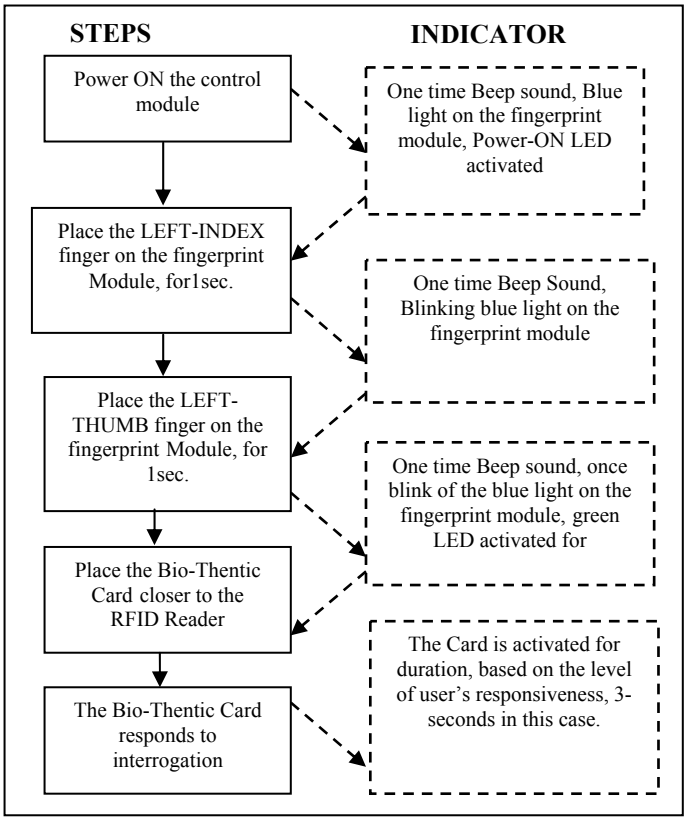


Figure 6a: Testing Procedure for Authentic User

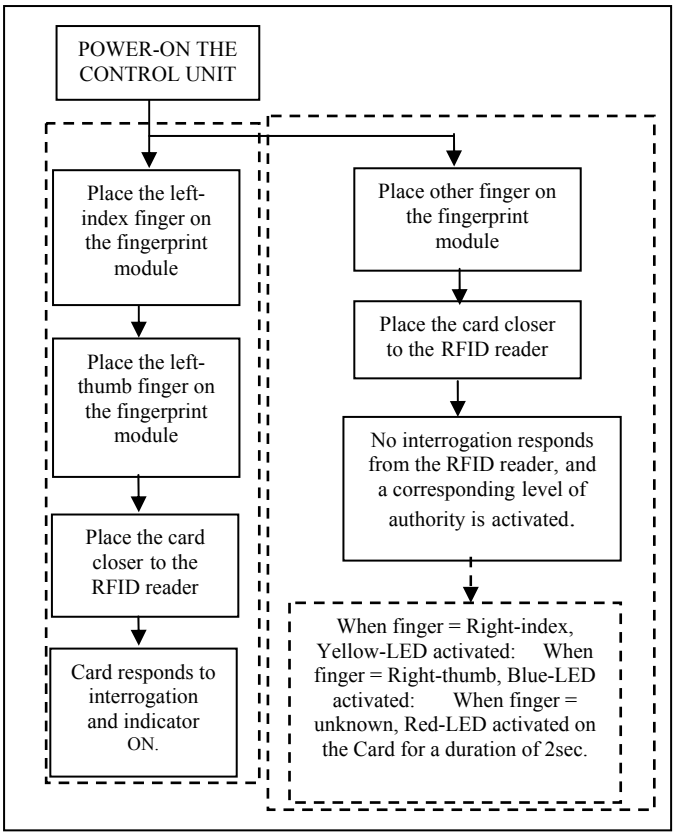


Figure 6b: Generic Testing Procedure

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VII. CONCLUSION

The main contribution of this paper is derived from the research carried out on authentication of an RFID card holder, on the card itself. This is predicated on the fact that the confidentiality of a system that adopts the use of RFID Card is vulnerable to unauthorized use. This paper therefore presents a concept of on-card authentication system as a preventive measure against unauthorized use of RFID Card. An on-card authentication system called Bio-Thentic card was designed, fabricated and evaluated. Furthermore, the Card was subjected to various known attacks, as a risk evaluation measure. The Bio-Thentic card proves to mitigate unauthorized Card use, and consequentially, prevents most known attacks against the RFID Card.

REFERENCES

[1]. Rubin, J. (2011, June 28). *Michael Faraday: The Invention of Faraday Cage.* Retrieved June 28, 2011, from Following the path of Discovery: http://www. juliantrubin. com/bigten/faradaycageexperiments. Html

[2]. Juels, A. (2006). RFID Security and Privacy: A Research Survey. *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS* , 381-394.

[3] Torstein, H. (2006). *Security and Privacy in RFID Applications.* NTNU.

[4]. A. Karygiannis, B. E. (2008). Practical Steps for Securing RFID Systems. In a. M. Syed Ahson, *RFID Handbook: Applications, Technology, security and privacy* (pp. 533-561). Boca Raton, FL: CRC Press .

[5]. Samuel Fosso Wamba, É. L.-A. (2008). From Automatic Identification and Data Capture to ‘‘Smart Business Process’’: Preparing for a Pilot Integrating RFID. In a M. Syed Ahson, *RFID Handbook: Application, technology, Security and Application* (pp. 279-294). Boca Raton, FL: CRC Press.

[6]. Haines, B. (2010). *Radio Frequency Identification Attacks.* Boston, , USA: Seven Deadliest Wireless Technologies Attacks, Syngress.

[7]. Peter J. Hawrylak, M. M. (2008). RFID Tags. In Y. Z. Lu Yan, *THE INTERNET OF THINGS* (pp. 14-45). London: Taylor & Francis Group, LLC.

[8]. Paul A. Moskowitz, A. L. (2007). A Privacy-Enhancing Radio Frequency Identification Tag:Implementation of the Clipped Tag. *IEEE International Conference* , 0-7695-2788-4/07 .

[9]. Aikaterini Mitrokotsa, M. R. (2010). Classification of RFID Attacks. *Information Systems Frontiers , 12* (5), 491-505.

[10]. Shang-Ping, W. (2011). An Authentication Protocol for RFID Tag and Its Simulation. *Journal of Network* , 446-453.

[11]. Feng Gao, J. T. (2008). An Algorithm to Produce Temporally and Spatially Continuous MODIS-LAI Time series. *Geoscience and Remote Sensing Letters,* (pp. 60-64). IEEE.

[12]. YUNG-CHIN CHEN, W. -L. W. -S. (2006). Low-Cost RFID Authentication Protocol for Anti-Counterfeiting and Privacy Protection. *Asian Journal of health and Information Science* , 189-203.

[13]. Y. -C. Lee, Y. -C. H. -S. -C. (2009). A New Ultralightweight RFID protocol with Mutual Authentication. *Information Engineering, 2009. ICIE '09. WASE International Conference* (pp. 58-61). IEEE.

[14]. Shang-Ping, W. (2011). An Authentication Protocol for RFID Tag and Its Simulation. *Journal of Network* , 446-453.

[15]. Mikko Lehtonen, T. S. (2008). From Identification to Authentication –A Review of RFID Product Authentication Techniques. In a. D. Peter H. Cole, *networked RFID Systems and Lightweight Cryptography: Barrier raising to counterfeinting* (pp. 168-187). Adelaide: Springer.

[16]. Ranasinghe1, D. C. (2008). Lightweight Cryptography for Low Cost RFID. In a. D. Peter H. Cole, *Networked RFID Systems, and LightWeight Cryptography* (pp. 311-346). Adelaide: Springer.

[17]. Juels, A. (2005). Strengthening EPC Tags Against Cloning. *Proceedings of the 4th ACM workshop on Wireless security* (pp. 67-75). ACM.

[15]. Mikko Lehtonen, T. S. (2008). From Identification to Authentication –A Review of RFID Product Authentication Techniques. In a. D. Peter H. Cole, *networked RFID Systems and Lightweight Cryptography: Barrier raising to counterfeinting* (pp. 168-187). Adelaide: Springer.

[16]. Ranasinghe1, D. C. (2008). Lightweight Cryptography for Low Cost RFID. In a. D. Peter H. Cole, *Networked RFID Systems, and LightWeight Cryptography* (pp. 311-346). Adelaide: Springer.

[18]. Damith C. Ranasinghe1, S. D. (2008). A Low Cost Solution to Cloning and Authentication Based on a Lightweight Primitive. In a. D. Peter H. Cole, *Networked RFID Systems and Lightweight Cryptography: raising Barriers to product counterfieting* (pp. 289-310). Adelaide: Springer.

[19]. Koutarou Suzuki, M. O. (2008). Cryptographic Approaches to RFID Security and Privacy. In a. M. Syed Ahson, *RFID Handbook Application, Technology, Security and privacy* (pp. 631-642). Boca Raton, FL: CRC Press.

[20]. Damith C. Ranasinghe, R. G. (2008). Lightweight Cryptography for Low Cost RFID: A New Direction in Cryptography. In a. M. Syed Ahson, *RFID Handbook Application, Technology, Security, and Privacy* (pp. 573-588). Boca Raton, FL: CRC Press.

[21]. Ari Juels, R. L. (2003,). The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. *Proceedings of the 10th ACM conference on Computer and communications security* (pp. 103-111). Was hington, DC,: ACM.

[22]. Melanie R. Rieback, B. C. (2005, July). RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. *Australasian Conference on Information Security and Privacy(ACISP).* , 62-69.

[23]. MiniMe, a. M. (2006, June 2). *rfid-zapper.* Retrieved June 2-15, 2011, from RFID-Zapper(EN): http://itp. nyu. edu/everybit/blog/media/

[24]. Paul A. Moskowitz, A. L. (2007). A Privacy-Enhancing Radio Frequency Identification Tag: Implementation of the Clipped Tag. *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference* (pp. 348-351). IEEE.

[25]. Yuhanim Hani Binti Yahaya, M. R. (2009). Fingerprint Biometrics Authentication on Smart Card. *ICCEE '09. Second International Conference on Computer and Electrical Engineering* (pp. 671-673). IEEE.

[26]. Chao Li, a. J. (2010). A Two-Factor Authentication Design of Fingerprint Recognition System Based on DSP and RF Card. *IEEE* (pp. 441-445). IEEE.

[27]. Nicolai Marquardt, A. S. (2010). Visible and Controllable RFID Tags. *'10: Proceedings of the 28th of the international conference extended abstracts on Human factors in computing* systems (pp. 3057-3062). Atlanta, GA, USA: ACM.

[28]. Yum, J. , Yoo, B. , Park, K. , & Jang, J. (2010). *Smart card with an integrated electrical switch for secure operation.* IEEE.

[29]. Davide zanetti, B. d. (2010). Physical-layer identification of UHF tags. *MobiCom '10: Proceedings of the sixteenth annual international conference on Mobile computing and networking* (pp. 978-1-4503-0181). Illinois,USA: ACM.

[30]. Joyce H. Wu, a. J. (2004). An Equivalent Circuit Model for a Faraday Cage Substrate Crosstalk Isolation Structure. *Radio Frequency Integrated Circuits (RFIC) Symposium* , pp. 0-7803-8333.

[31]. Adeyemi R. and Norafida I.(2012). Users Authentication of RFID Card. Unpublished article Universiti Teknologi, Malaysia.

ARP Cache Poisoning Attack and Detection

Fatimah mohammed Al-Qarni
07120229
Computer Science and Engineering
Yanbu University College
fatimah.mail@hotmail.com

1. Introduction

One of the most prevalent network attacks used against individuals and large organizations alike are man-in-the-middle (MITM) attacks. Considered an active eavesdropping attack, MITM works by establishing connections to victim machines and relaying messages between them. In cases like these, one victim believes it is communicating directly with another victim, when in reality the communication flows through the host performing the attack. The end result is that the attacking host can not only intercept sensitive data, but can also inject and manipulate a data stream to gain further control of its victims [1].

The address resolution protocol (ARP) is a TCP/IP protocol used by computers to map network addresses (IP) to physical addresses (MAC). The protocol has proved to work well under regular circumstances, but it was not designed to cope with malicious hosts. By performing ARP cache poisoning or ARP spoofing attacks, an intruder can impersonate another host MITM.

The paper is organized as follows: In first section, we give a detailed description of ARP cache poisoning. Then, we show how ARP cache poisoning attack can be conducted using Cain and Abel, how password stealing and phishing can be conducted through ARP cache poisoning, how XArp is used to detect ARP cache poisoning attack, and how ARP Freeze is used to prevent ARP cache poisoning attack. Finally, we conclude.

2. ARP Cache Poisoning

In the first section of this paper we will take a look at ARP cache poisoning. One of the oldest forms of modern MITM attack, ARP cache poisoning (sometimes also known as ARP Poison Routing) allows an attacker on the same subnet as its victims to eavesdrop on all network traffic between the victims. It is one of the simplest to execute but is considered one of the most effective once implemented by attackers [2].

2.1. Normal ARP Communication

The ARP protocol was designed out of necessity to facilitate the translation of addresses between the second and third layers of the OSI model. The second layer, or data-link layer, uses MAC addresses so that hardware devices can communicate to each other directly on a small scale. The third layer, or network layer, uses IP addresses (most commonly) to create large scalable networks that can communicate across the globe. The data link layer deals directly with devices connected together where as the network layer deals with devices that are directly connected AND indirectly connected. Each layer has its

own addressing scheme, and they must work together in order to make network communication happen. For this very reason, ARP was created with RFC 826, "An Ethernet Address Resolution Protocol" [10].

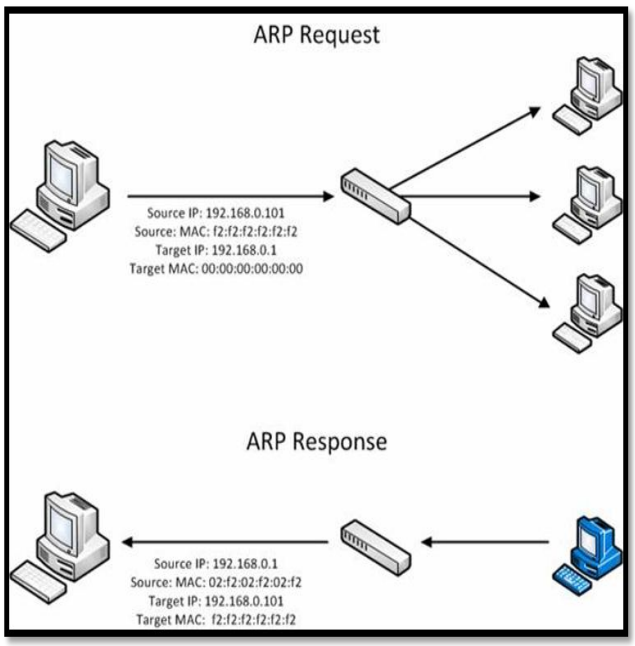


Figure 1: The ARP Communication Process.

The nitty gritty of ARP operation is centered around two packets, an ARP request and an ARP reply. The purpose of the request and reply are to locate the hardware MAC address associated with a given IP address so that traffic can reach its destination on a network. The request packet is sent to every device on the network segment and says "Hey, my IP address is XX.XX.XX.XX, and my MAC address is XX:XX:XX:XX:XX:XX. I need to send something to whoever has the IP address XX.XX.XX.XX, but I don't know what their hardware address is. Will whoever has this IP address please respond back with their MAC address?" The response would come in the ARP reply packet and effectively provide this answer, "Hey transmitting device. I am who you are looking for with the IP address of XX.XX.XX.XX. My MAC address is XX:XX:XX:XX:XX:XX." Once this is completed the transmitting device will update its ARP cache table and the devices are able to communicate with one another [6], [11].

2.2. Poisoning the Cache

ARP cache poisoning takes advantage of the insecure nature of the ARP protocol. Unlike protocols such as DNS that can be configured to only accept secured dynamic updates, devices using ARP will accept updates at any time. This means that any device can send an ARP reply packet to another host and force that host to update its ARP cache with the new value. Sending an ARP reply when no request has been generated is called sending a gratuitous ARP. When malicious intent is present the result of a few well placed gratuitous ARP packets used in this manner can result in hosts who think they are communicating with one host, but in reality are communicating with a listening attacker [12].

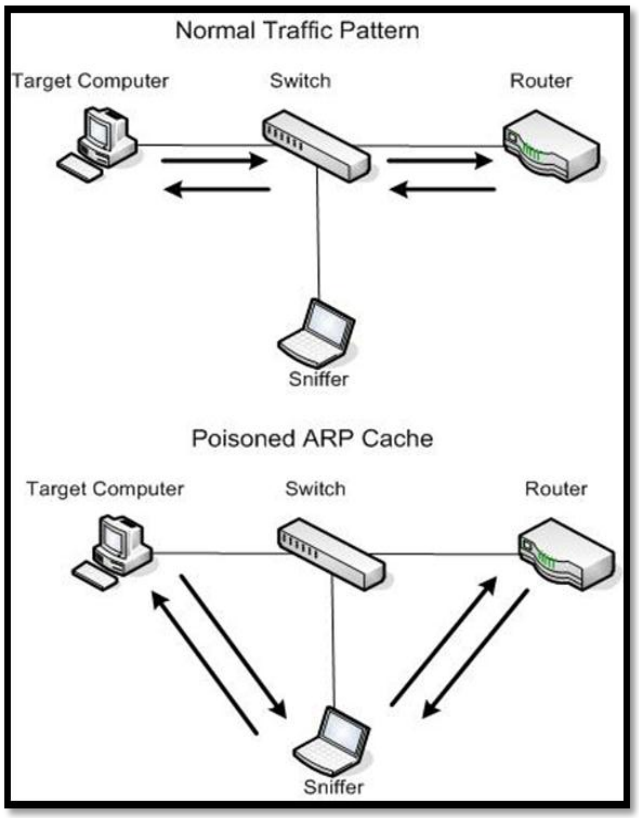


Figure 2: Intercepting Communication with ARP Cache Poisoning.

3. ARP Cache Poisoning Attack and Detection

ARP cache poisoning attacks allow an attacker to silently eavesdrop or manipulate all your data that is sent over the network. This includes documents, emails and VoiceIP conversations.
ARP spoofing attacks are undetected by firewalls and operating system security features [9].

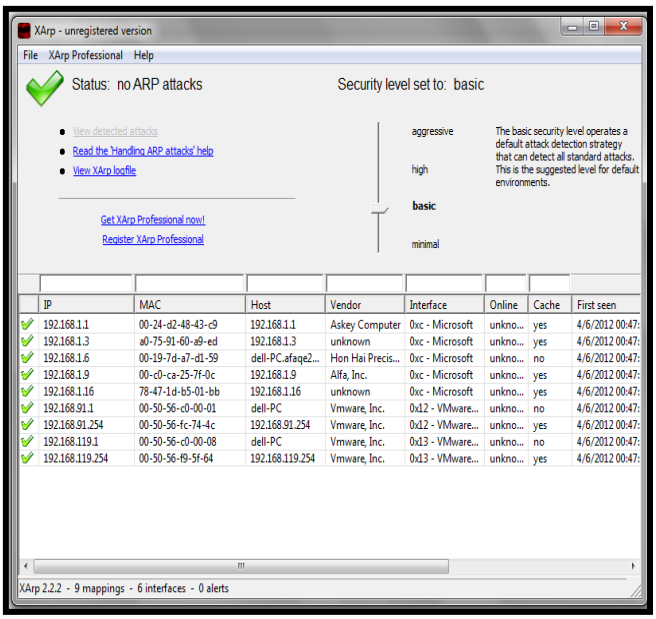
3.1. Using Cain & Abel and XArp tools

Let us take the given scenario above and take it from theory to reality. There are a few different tools that will perform the necessary steps to poison the ARP cache of victim machines. We will use the popular security tool Cain & Abel from Oxid.it [3]. Cain and Abel does quite a few things beyond ARP cache poisoning and is a very useful tool to have in your arsenal.

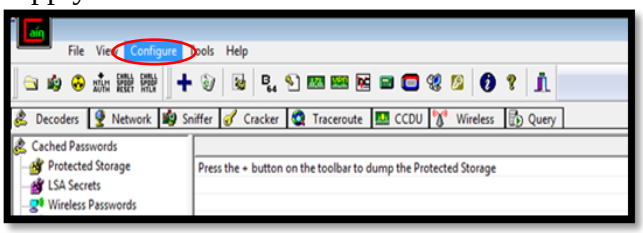
XArp [4] is a security application that uses advanced techniques to detect ARP based attacks. As we said firewalls don't protect you against ARP based attack! So, XArp has been developed to target this problem: it uses advanced techniques to detect ARP attacks and thus helps you to keep your data private. If a potential threat is detected, the program alerts you via pop-up message on your desktop.

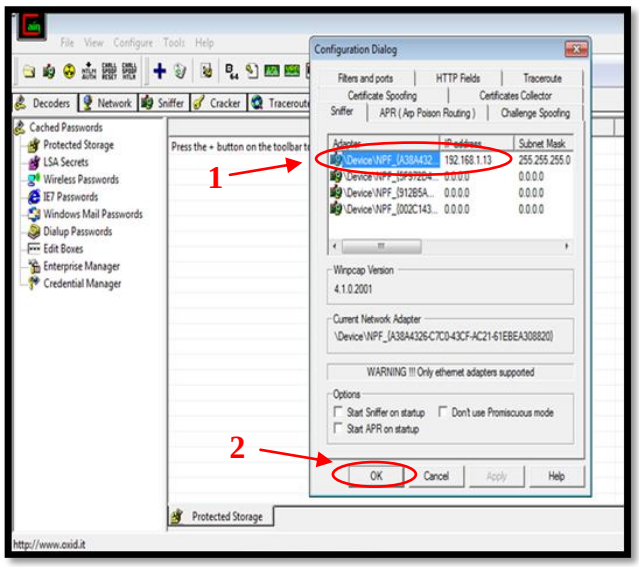
Now, let us show you how ARP cache poisoning attacks conducted using Cain and Abel, how password stealing and phising done by ARP poisoning and how XArp is used to detect it.
You need to use two laptops and connect it wirelessly. One is the attacker's computer; the other is the victim's computer. Install Cain & Abel on the attacker computer.
Then follow these procedures:

1) Run XArp on the victim's computer.

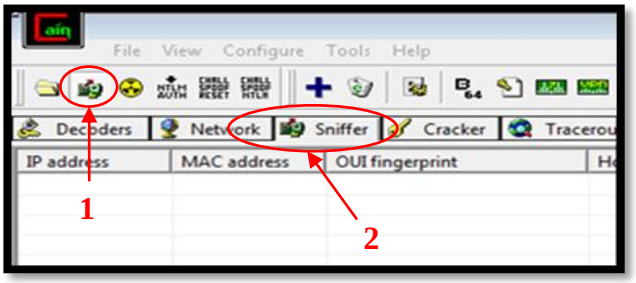


2) Open Cain & Abel on the attacker's computer. At main screen, select Configure, then click your network adapter, then Apply and Ok.

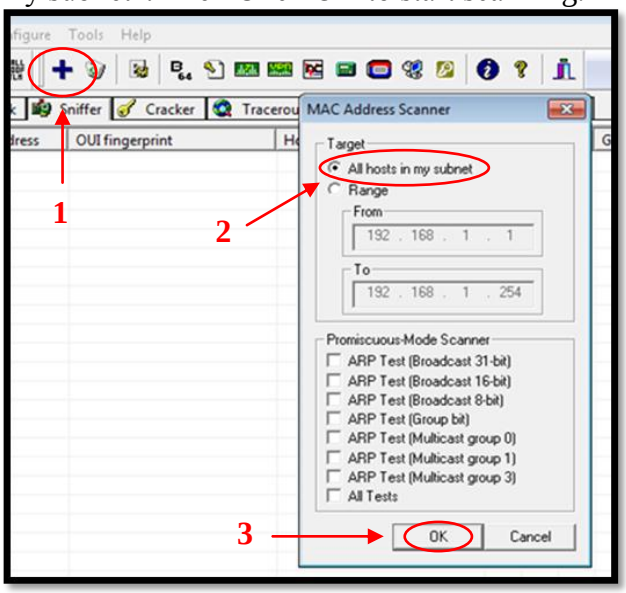




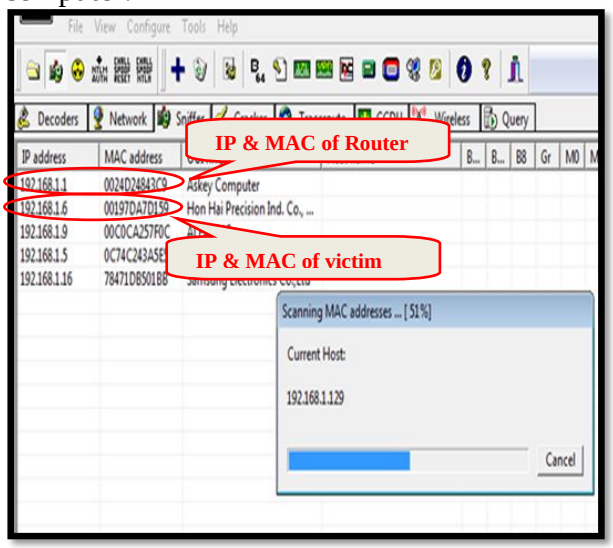
3) Click to enable Sniffer and go to sniffer tab.



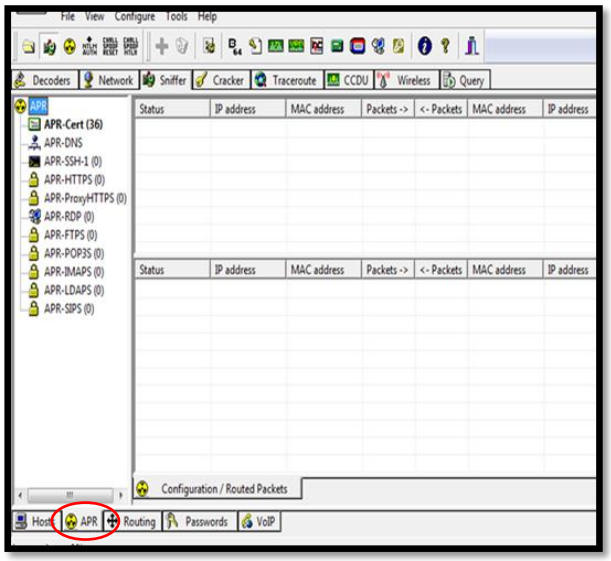
4) Click on blue + icon and select "All Hosts in my subnet". Then Click OK to start scanning.



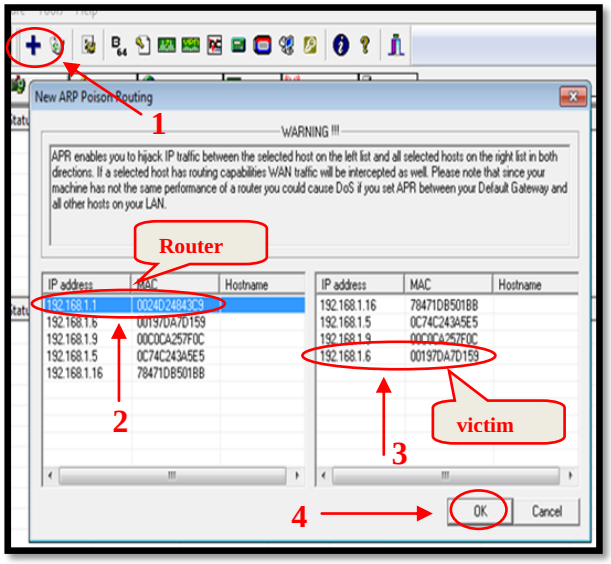
After 100% you will see IP address, MAC address, and OUI fingerprint of devices. Two IP addresses should be displayed. One is the router/gateway; the other is the victim's computer.



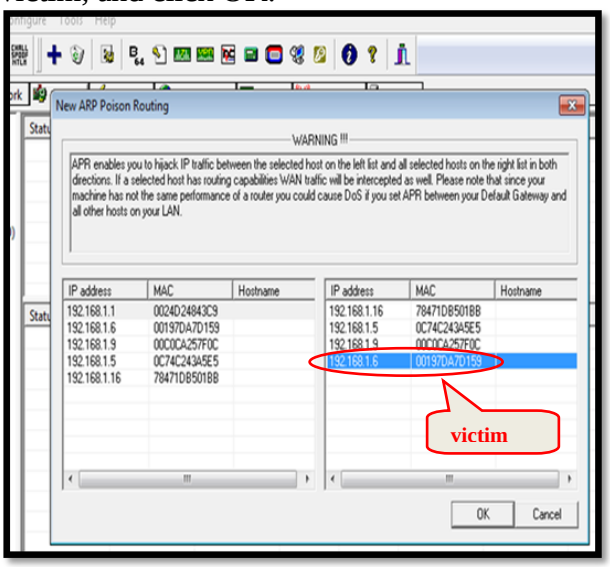
5) Now click on APR tab at the bottom to enable it.



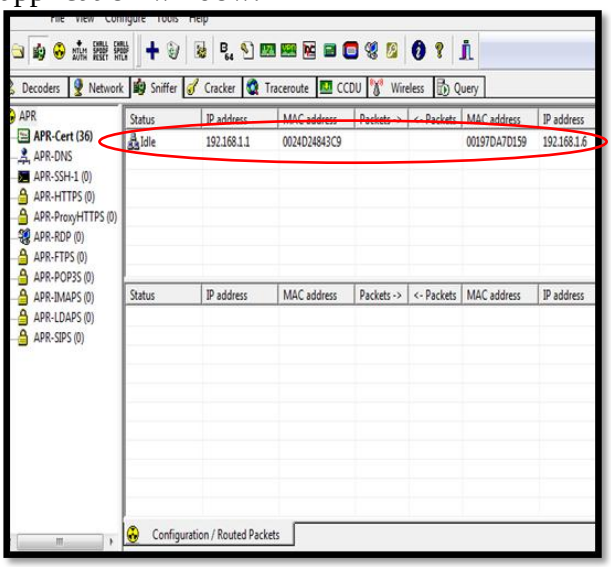
Click on the top field and then click on the blue + icon. The window that appears has two selection columns side by side. On the left side, the IP address should be the router. Click the IP address. This will result in the right window showing a list of all hosts in the network (the victim's computer) then OK.



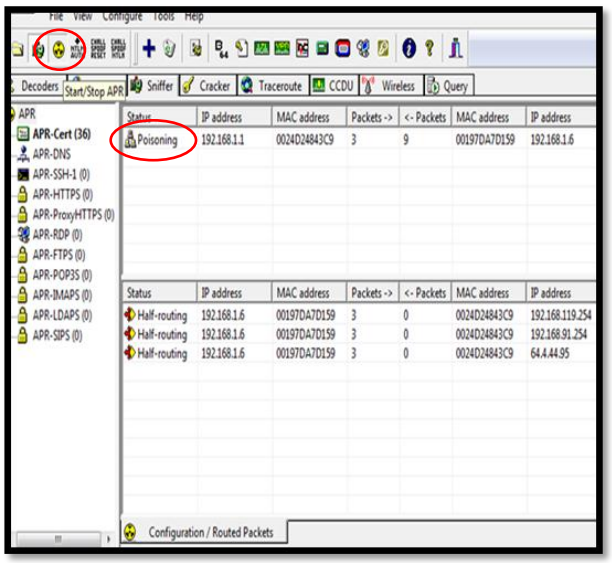
In the right window, click the IP address of the victim, and click OK.



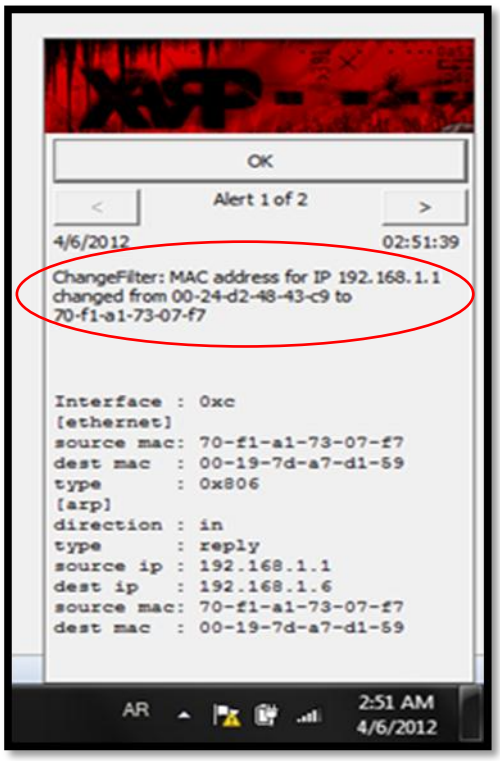
6) The IP addresses of the victim should now be listed in the upper table in the main application window.

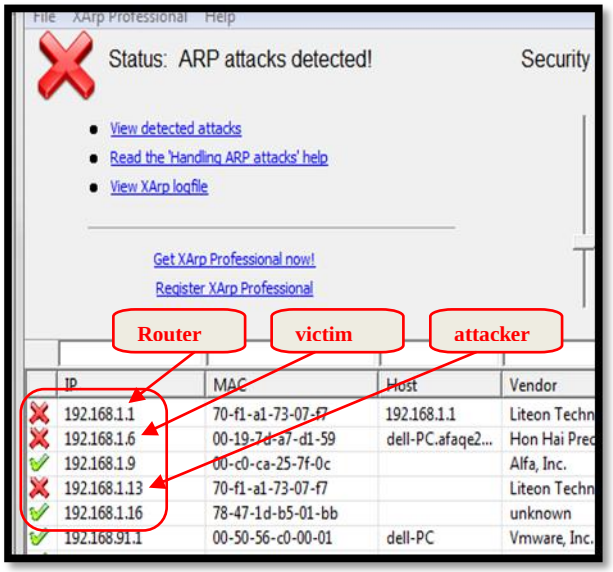


To complete the process, click the yellow-and-black radiation symbol on the standard toolbar. This will activate Cain and Abel's ARP cache poisoning features and allow your analyzing system to be the middleman for all communications between the two victims.

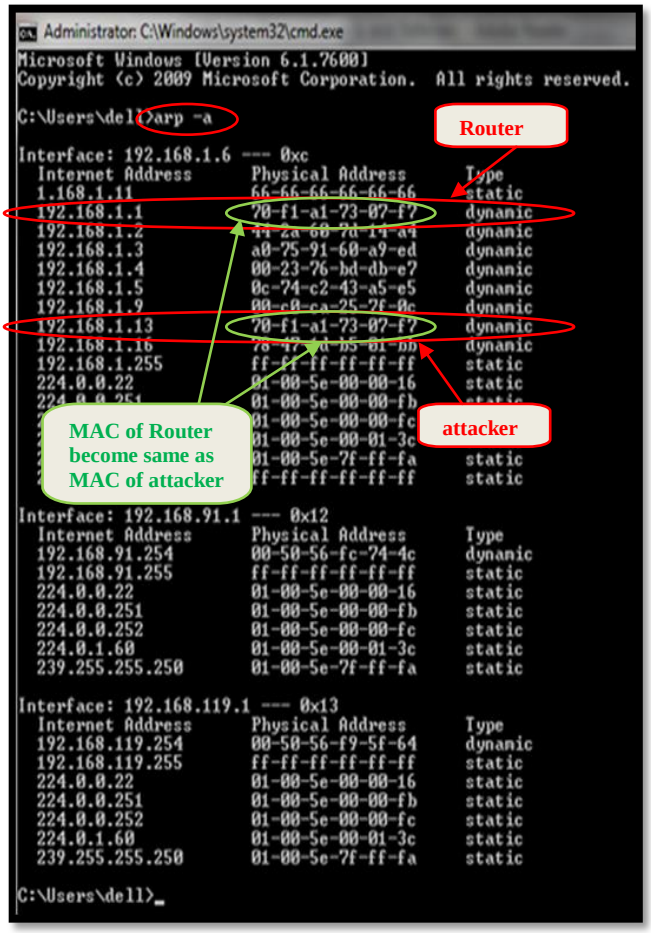


7) Now, at the same time on the victim's computer, the XArp program will display an alert window on the lower right hand corner of the screen to inform the user that ARP cache poisoning attack has occurred.



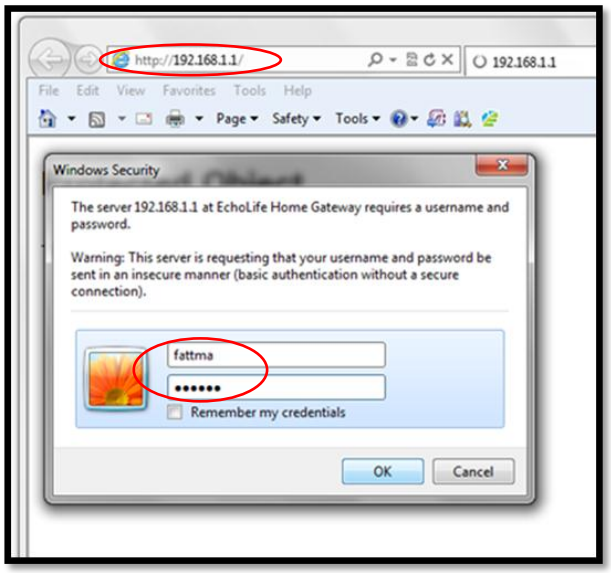


8) On the victim's computer, open the Command Line prompt window and write "arp –a". You will see an entry that has the IP address of the router and the MAC address of the attacker in the ARP cache.

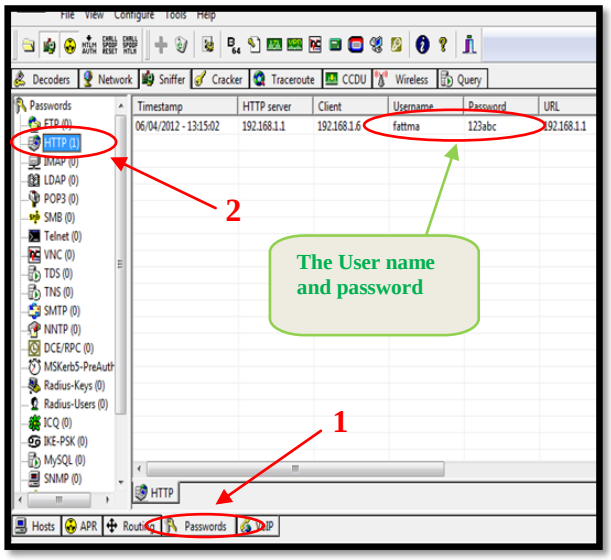


ARP cache poisoning can also be used to steel passwords, the following procedure demonstrate that:

9) Open the web browser on the victim's computer, go to the address bar and write this: http://<router's IP> (i.e., http://192.168.1.1). Then log into the configuration page.



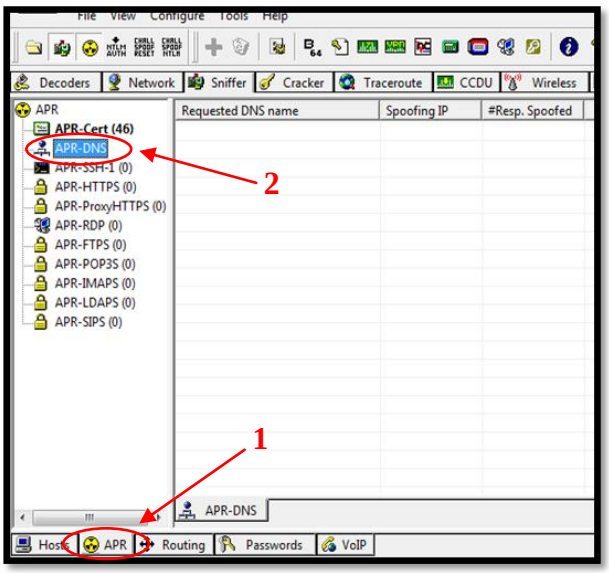
10) Now, on the attacker's computer, click the Passwords tab at the bottom. Select the HTTP option on the left. The username and password information used by the victim will be displayed in the list.



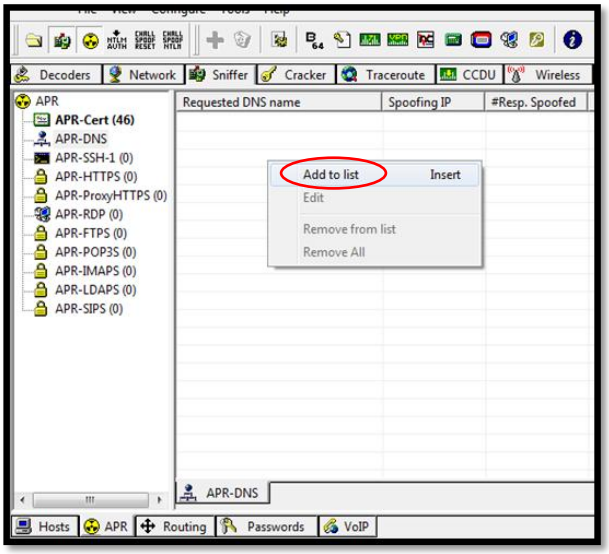
The above steps show how to intercept HTTP username and passwords.

ARP cache poisoning can also be used to conduct phishing, the following procedure demonstrates that:

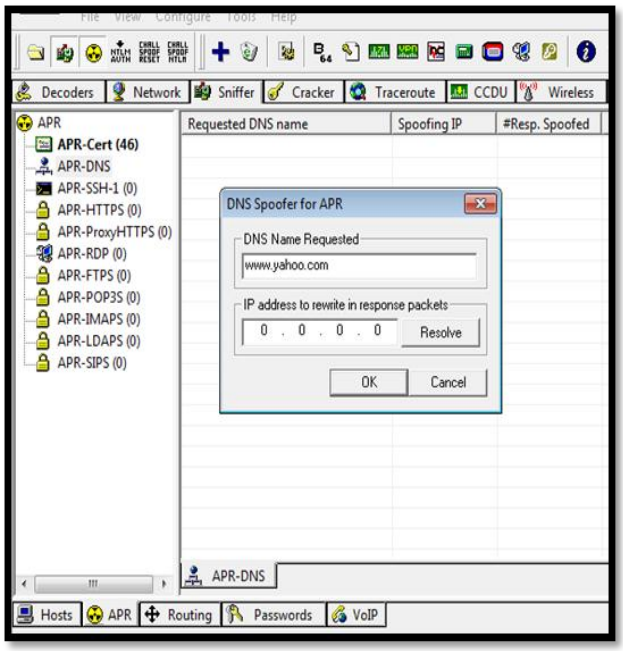
11) On the attacker's computer, click on the APR tab at bottom then go to the left panel and click on the "APR-DNS".



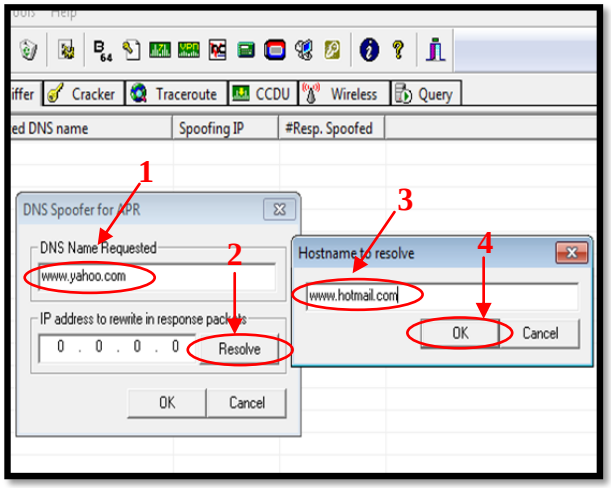
12) Do right click and then choose "add to the list".



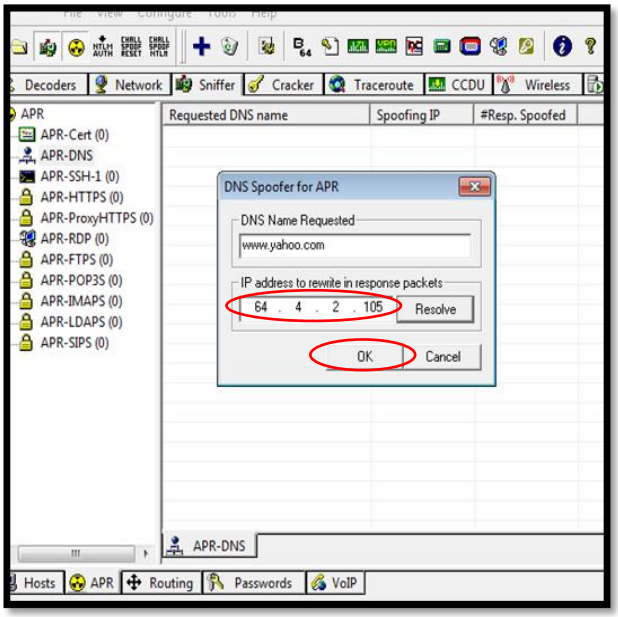
The following "DNS Spoofer for APR" window will appear:



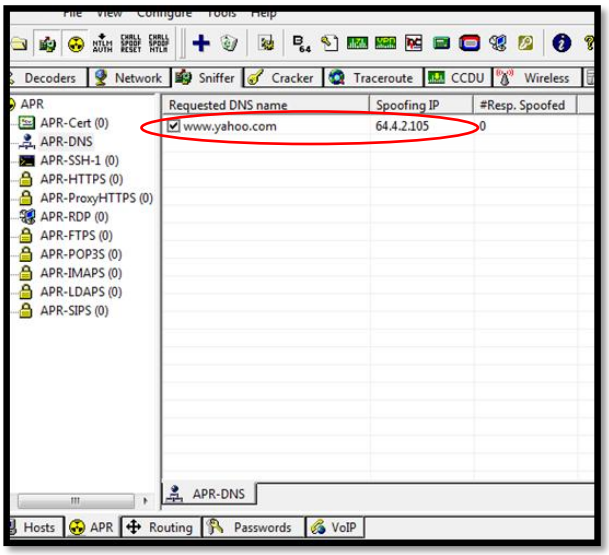
13) For our test run, let's hijack the traffic from www.yahoo.com . So, type www.yahoo.com in the "DNS Name Requested" box. Since you are not sure of what the IP address you want to redirect to is, click on the "Resolve" box. What you will do is redirect the traffic from www.yahoo.com to www.hotmail.com. So, type www.hotmail.com in "Hostname to resolve" box and click OK.



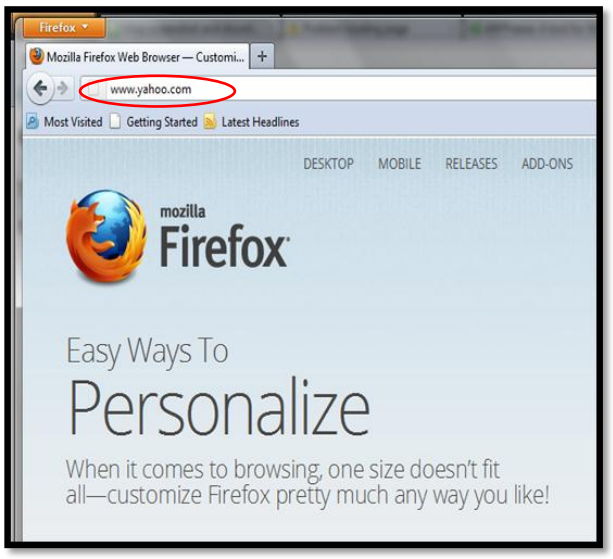
14) The IP should resolve and we should now have the IP address of www.hotmail.com. Click OK.



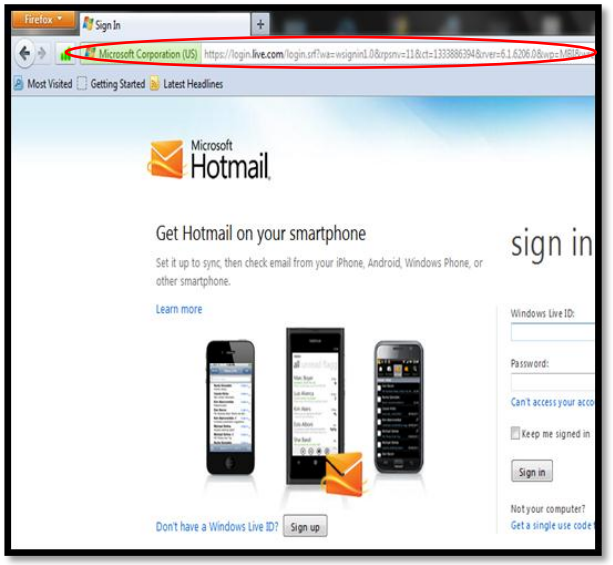
So, now you should have the DNS name spoofed.



15) On the victim's computer, open the browser and go to www.yahoo.com to see if APR-DNS poison routing worked.



As you can see, when you type www.yahoo.com you ended up at www.hotmail.com.



4. ARP Cache Poisoning Prevention

Looking at ARP cache poisoning from the defenders standpoint we are at a bit of a disadvantage. The ARP process happens in the background with very little ability to be controlled directly by us. There is no catch all solution, but proactive and reactive stances can

be taken if you are concerned about ARP cache poisoning on your network [7].

4.1. Securing the LAN

ARP Cache Poisoning is only a viable attack technique when attempting to intercept traffic between two hosts on the same local area network. The only reason you would have to fear this is if a local device on your network has been compromised, a trusted user has malicious intent, or someone has managed to plug an un-trusted device into the network. Although we too often focus the entirety of our security efforts on the network perimeter, defending against internal threats and having a good internal security posture can help eliminate the fear of the attack mentioned here.

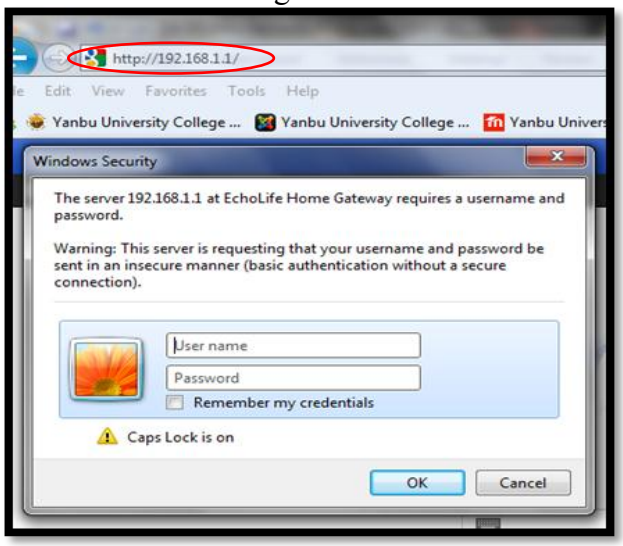
4.2. Using ARP Freeze tool

Here let us show you how ARP Freeze [5] is used to prevent ARP cache poisoning attack ARPFreeze is a tool for prevention. It lets you setup static ARP tables so that other attackers (using Cain and abel or some other tool) can't pull off an ARP poisoning attack against you. Windows has tools built in for doing this (the arp command) but these are not easy or automated, so using ARPFreeze, a simple automation script. It looks at your current ARP table, and lets you make entries static. It may help someone in hardening a box against Man in the Middle attacks that use ARP poisoning.

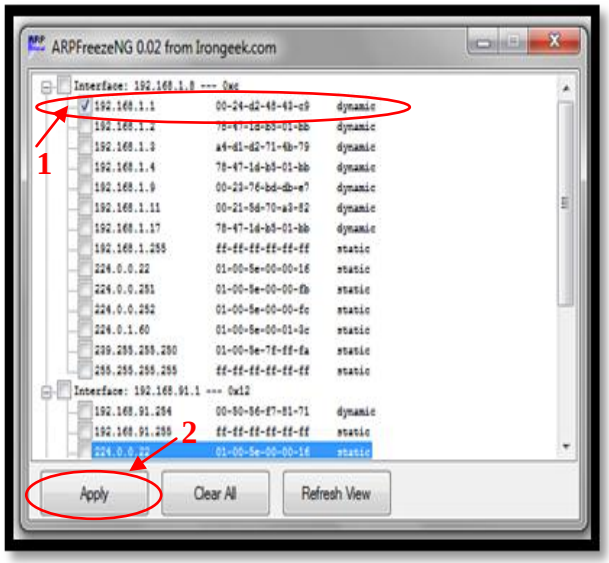
To continue from the above steps, the following steps can be followed to demonstrate the ARP cache poisoning prevention method using static ARP routing:

16) Close Cain and Abel on the attacker's computer.

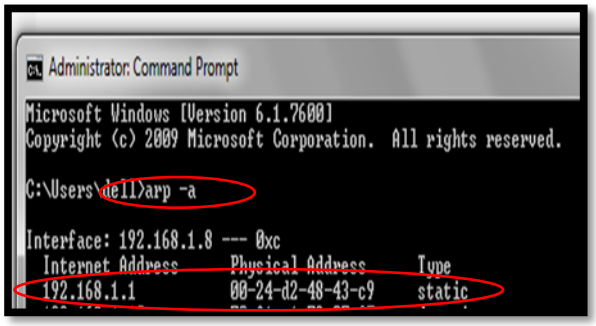
17) Open the browser on the victim's computer and type the IP address of the router to go to the router configuration page. This will update the victim's ARP cache with the router's IP address again.



18) Open ARP Freeze on the victim's computer. ARP Freeze displays the current ARP cache and for each entry will ask if you want that entry to become static or not. Click Yes for the entry that has the router (IP address). Click No for all other entries.

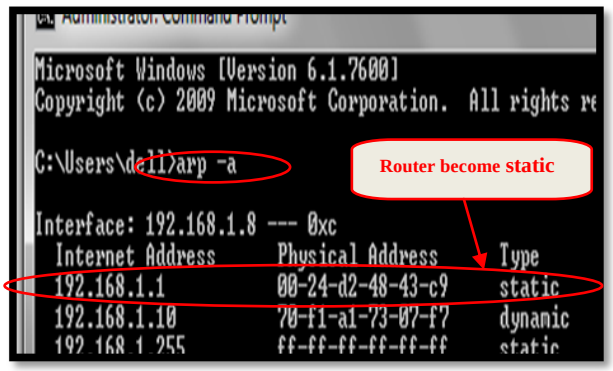


19) On the victim's computer, open the command line window again and type "arp –a" to view the ARP cache.

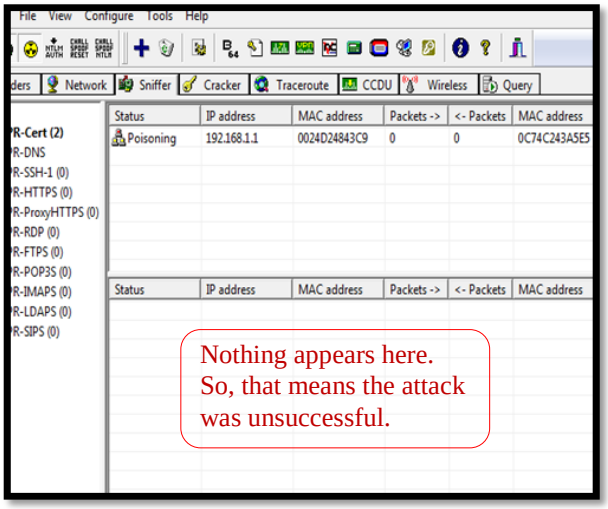


20) Repeat steps (2) – (6) on the attacker's computer to conduct the ARP cache poisoning process again.

21) On the victim's computer again, open the command line window and type "arp –a" to view the ARP cache. Notice that the ARP entry for the router is unchanged.



Although Cain and Abel say it's poisoning, the victim was not poisoned and therefore the attack was unsuccessful.



4.3. Monitoring ARP Traffic with a Third Party Program

The last option for defending against ARP cache poisoning is a reactive approach that involves monitoring the network traffic of hosts. This can be done through downloadable utilities designed specifically for this purpose (such as XArp) as we used and explained in previous section of this paper. This may be feasible when you are only concerned about a single host, but can be a bit cumbersome to deal with when concerned with entire network segments.

5. Conclusion

The security problems that the use of ARP introduces in a local area network (LAN) may create vulnerabilities to the distributed systems that run on these networks. Due to the severity of this problem, several ways to mitigate detect and prevent ARP attacks have been proposed, but each has its limitations.

In this report we have shown how ARP cache poisoning attack can be conducted using Cain and Abel, how password stealing and phishing can be conducted through ARP cache poisoning, how XArp is used to detect ARP cache poisoning attack, and how ARP Freeze is used to prevent ARP cache poisoning attack.

It is expected that from a small proof of concept as our study, a mechanism can be developed to be applied for future networks to prevent further attacks that can occur as a result of an ARP poisoning.

6. Recommends

We recommend that the student must take labs in security course to support the theoretical part

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

of the course, and understand the concepts better by performing it.

This practice makes them aware of contemporary security threats and what they need to do to counter them.

Also, we recommend designing comprehensive laboratory exercises to help the student learn how to apply security principles and tools in practice.

Finally, we recommend making the work and analysis as a group, so the students can share their experiences and knowledge with each other.

7. References

[1] Ramy Al Damaty. (2010). *understanding-man-in-middle-attacks.* Retrieved April 11, 2012, from

http://ramydamaty.blogspot.com/2010/06/understanding-man-in-middle-attacks_20.html

[2] Brushi, D., Ornaghi, A., Rosti, E. (2003), *S-ARP: A Secure Address Resolution Protocol.*

[3] Cain and Abel v4.9.14.
http://www.oxid.it/cain.html

[4] XArp,
http://free-software.tt5r.com/soft9513.html

[5] ARP Freeze,
http://www.dl4all.com/rpf/tag/arp+freeze.html

[6] Whalen, s.(2001). *An introduction to ARP spoofing.* Retrieved March 20, 2012, from

http://servv89pn0aj.sn.sourcedns.com.

[7] Tripunithara, M.V., Dutta, P. (1999). *A Middleware Approach to Asynchronous and Backward Compatible Detection and Prevention of ARP Cache Poisoning.*

[8] *Technical Interview Questions – Networking*. (n.d.). Retrieved April 19, 2012, From

http://dc166.4shared.com/doc/AAX9Z58A/preview.html

[9] Nir Sofer (2005). *SniffPass v1.12 - Password Monitoring.* Retrieved March 23, 2012, From

http://www.nirsoft.net/utils/password_sniffer.html

[10] Droms, R. *Dynamic Host Configuration Protocol, RFC2131*

[11] Fleck, B., Dimov, J., *Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network.* Retrieved March 23, 2012, From

http://www.eecs.umich.edu/~aprakash/eecs588/handouts/arppoison.pdf

[12] T. Demuth and A. Leitner. (2005). *ARP spoofing and poisoning: Traffic tricks.*

IJCSIS REVIEWERS' LIST

Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway
Assoc. Prof. N. Jaisankar, VIT University, Vellore,Tamilnadu, India
Dr. Amogh Kavimandan, The Mathworks Inc., USA
Dr. Ramasamy Mariappan, Vinayaka Missions University, India
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India
Dr Genge Bela, "Petru Maior" University of Targu Mures, Romania
Dr. Junjie Peng, Shanghai University, P. R. China
Dr. Ilhem LENGLIZ, HANA Group - CRISTAL Laboratory, Tunisia
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India
Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain
Prof. Dr.C.Suresh Gnana Dhas, Anna University, India
Mrs Li Fang, Nanyang Technological University, Singapore
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Dr. Siddhivinayak Kulkarni, University of Ballarat, Ballarat, Victoria, Australia
Dr. A. Arul Lawrence, Royal College of Engineering & Technology, India
Mr. Wongyos Keardsri, Chulalongkorn University, Bangkok, Thailand
Mr. Somesh Kumar Dewangan, CSVTU Bhilai (C.G.)/ Dimat Raipur, India
Mr. Hayder N. Jasem, University Putra Malaysia, Malaysia
Mr. A.V.Senthil Kumar, C. M. S. College of Science and Commerce, India
Mr. R. S. Karthik, C. M. S. College of Science and Commerce, India
Mr. P. Vasant, University Technology Petronas, Malaysia
Mr. Wong Kok Seng, Soongsil University, Seoul, South Korea
Mr. Praveen Ranjan Srivastava, BITS PILANI, India
Mr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong
Mr. Mohd Nazri Ismail, Universiti Kuala Lumpur, Malaysia
Dr. Rami J. Matarneh, Al-isra Private University, Amman, Jordan
Dr Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria
Dr. Riktesh Srivastava, Skyline University, UAE
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt
and Department of Computer science, Taif University, Saudi Arabia
Mr. Tirthankar Gayen, IIT Kharagpur, India
Ms. Huei-Ru Tseng, National Chiao Tung University, Taiwan

Prof. Ning Xu, Wuhan University of Technology, China
Mr Mohammed Salem Binwahlan, Hadhramout University of Science and Technology, Yemen
& Universiti Teknologi Malaysia, Malaysia.
Dr. Aruna Ranganath, Bhoj Reddy Engineering College for Women, India
Mr. Hafeezullah Amin, Institute of Information Technology, KUST, Kohat, Pakistan
Prof. Syed S. Rizvi, University of Bridgeport, USA
Mr. Shahbaz Pervez Chattha, University of Engineering and Technology Taxila, Pakistan
Dr. Shishir Kumar, Jaypee University of Information Technology, Wakanaghat (HP), India
Mr. Shahid Mumtaz, Portugal Telecommunication, Instituto de Telecomunicações (IT) , Aveiro, Portugal
Mr. Rajesh K Shukla, Corporate Institute of Science & Technology Bhopal M P
Dr. Poonam Garg, Institute of Management Technology, India
Mr. S. Mehta, Inha University, Korea
Mr. Dilip Kumar S.M, University Visvesvaraya College of Engineering (UVCE), Bangalore University, Bangalore
Prof. Malik Sikander Hayat Khiyal, Fatima Jinnah Women University, Rawalpindi, Pakistan
Dr. Virendra Gomase , Department of Bioinformatics, Padmashree Dr. D.Y. Patil University
Dr. Irraivan Elamvazuthi, University Technology PETRONAS, Malaysia
Mr. Saqib Saeed, University of Siegen, Germany
Mr. Pavan Kumar Gorakavi, IPMA-USA [YC]
Dr. Ahmed Nabih Zaki Rashed, Menoufia University, Egypt
Prof. Shishir K. Shandilya, Rukmani Devi Institute of Science & Technology, India
Mrs.J.Komala Lakshmi, SNR Sons College, Computer Science, India
Mr. Muhammad Sohail, KUST, Pakistan
Dr. Manjaiah D.H, Mangalore University, India
Dr. S Santhosh Baboo, D.G.Vaishnav College, Chennai, India
Prof. Dr. Mokhtar Beldjehem, Sainte-Anne University, Halifax, NS, Canada
Dr. Deepak Laxmi Narasimha, Faculty of Computer Science and Information Technology, University of Malaya, Malaysia
Prof. Dr. Arunkumar Thangavelu, Vellore Institute Of Technology, India
Mr. M. Azath, Anna University, India
Mr. Md. Rabiul Islam, Rajshahi University of Engineering & Technology (RUET), Bangladesh
Mr. Aos Alaa Zaidan Ansaef, Multimedia University, Malaysia
Dr Suresh Jain, Professor (on leave), Institute of Engineering & Technology, Devi Ahilya University, Indore (MP) India,
Dr. Mohammed M. Kadhum, Universiti Utara Malaysia
Mr. Hanumanthappa. J. University of Mysore, India
Mr. Syed Ishtiaque Ahmed, Bangladesh University of Engineering and Technology (BUET)
Mr Akinola Solomon Olalekan, University of Ibadan, Ibadan, Nigeria
Mr. Santosh K. Pandey, Department of Information Technology, The Institute of Chartered Accountants of India
Dr. P. Vasant, Power Control Optimization, Malaysia
Dr. Petr Ivankov, Automatika - S, Russian Federation

Dr. Utkarsh Seetha, Data Infosys Limited, India
Mrs. Priti Maheshwary, Maulana Azad National Institute of Technology, Bhopal
Dr. (Mrs) Padmavathi Ganapathi, Avinashilingam University for Women, Coimbatore
Assist. Prof. A. Neela madheswari, Anna university, India
Prof. Ganesan Ramachandra Rao, PSG College of Arts and Science, India
Mr. Kamanashis Biswas, Daffodil International University, Bangladesh
Dr. Atul Gonsai, Saurashtra University, Gujarat, India
Mr. Angkoon Phinyomark, Prince of Songkla University, Thailand
Mrs. G. Nalini Priya, Anna University, Chennai
Dr. P. Subashini, Avinashilingam University for Women, India
Assoc. Prof. Vijay Kumar Chakka, Dhirubhai Ambani IICT, Gandhinagar ,Gujarat
Mr Jitendra Agrawal, : Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal
Mr. Vishal Goyal, Department of Computer Science, Punjabi University, India
Dr. R. Baskaran, Department of Computer Science and Engineering, Anna University, Chennai
Assist. Prof, Kanwalvir Singh Dhindsa, B.B.S.B.Engg.College, Fatehgarh Sahib (Punjab), India
Dr. Jamal Ahmad Dargham, School of Engineering and Information Technology, Universiti Malaysia Sabah
Mr. Nitin Bhatia, DAV College, India
Dr. Dhavachelvan Ponnurangam, Pondicherry Central University, India
Dr. Mohd Faizal Abdollah, University of Technical Malaysia, Malaysia
Assist. Prof. Sonal Chawla, Panjab University, India
Dr. Abdul Wahid, AKG Engg. College, Ghaziabad, India
Mr. Arash Habibi Lashkari, University of Malaya (UM), Malaysia
Mr. Md. Rajibul Islam, Ibnu Sina Institute, University Technology Malaysia
Professor Dr. Sabu M. Thampi, .B.S Institute of Technology for Women, Kerala University, India
Mr. Noor Muhammed Nayeem, Université Lumière Lyon 2, 69007 Lyon, France
Dr. Himanshu Aggarwal, Department of Computer Engineering, Punjabi University, India
Prof R. Naidoo, Dept of Mathematics/Center for Advanced Computer Modelling, Durban University of Technology, Durban,South Africa
Prof. Mydhili K Nair, M S Ramaiah Institute of Technology(M.S.R.I.T), Affliliated to Visweswaraiah Technological University, Bangalore, India
M. Prabu, Adhiyamaan College of Engineering/Anna University, India
Mr. Swakkhar Shatabda, Department of Computer Science and Engineering, United International University, Bangladesh
Dr. Abdur Rashid Khan, ICIT, Gomal University, Dera Ismail Khan, Pakistan
Mr. H. Abdul Shabeer, I-Nautix Technologies,Chennai, India
Dr. M. Aramudhan, Perunthalaivar Kamarajar Institute of Engineering and Technology, India
Dr. M. P. Thapliyal, Department of Computer Science, HNB Garhwal University (Central University), India
Dr. Shahaboddin Shamshirband, Islamic Azad University, Iran
Mr. Zeashan Hameed Khan, : Université de Grenoble, France
Prof. Anil K Ahlawat, Ajay Kumar Garg Engineering College, Ghaziabad, UP Technical University, Lucknow
Mr. Longe Olumide Babatope, University Of Ibadan, Nigeria
Associate Prof. Raman Maini, University College of Engineering, Punjabi University, India

Dr. Maslin Masrom, University Technology Malaysia, Malaysia
Sudipta Chattopadhyay, Jadavpur University, Kolkata, India
Dr. Dang Tuan NGUYEN, University of Information Technology, Vietnam National University - Ho Chi Minh City
Dr. Mary Lourde R., BITS-PILANI Dubai , UAE
Dr. Abdul Aziz, University of Central Punjab, Pakistan
Mr. Karan Singh, Gautam Budtha University, India
Mr. Avinash Pokhriyal, Uttar Pradesh Technical University, Lucknow, India
Associate Prof Dr Zuraini Ismail, University Technology Malaysia, Malaysia
Assistant Prof. Yasser M. Alginahi, College of Computer Science and Engineering, Taibah University, Madinah Munawwarrah, KSA
Mr. Dakshina Ranjan Kisku, West Bengal University of Technology, India
Mr. Raman Kumar, Dr B R Ambedkar National Institute of Technology, Jalandhar, Punjab, India
Associate Prof. Samir B. Patel, Institute of Technology, Nirma University, India
Dr. M.Munir Ahamed Rabbani, B. S. Abdur Rahman University, India
Asst. Prof. Koushik Majumder, West Bengal University of Technology, India
Dr. Alex Pappachen James, Queensland Micro-nanotechnology center, Griffith University, Australia
Assistant Prof. S. Hariharan, B.S. Abdur Rahman University, India
Asst Prof. Jasmine. K. S, R.V.College of Engineering, India
Mr Naushad Ali Mamode Khan, Ministry of Education and Human Resources, Mauritius
Prof. Mahesh Goyani, G H Patel Collge of Engg. & Tech, V.V.N, Anand, Gujarat, India
Dr. Mana Mohammed, University of Tlemcen, Algeria
Prof. Jatinder Singh, Universal Institutiion of Engg. & Tech. CHD, India
Mrs. M. Anandhavalli Gauthaman, Sikkim Manipal Institute of Technology, Majitar, East Sikkim
Dr. Bin Guo, Institute Telecom SudParis, France
Mrs. Maleika Mehr Nigar Mohamed Heenaye-Mamode Khan, University of Mauritius
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Mr. V. Bala Dhandayuthapani, Mekelle University, Ethiopia
Dr. Irfan Syamsuddin, State Polytechnic of Ujung Pandang, Indonesia
Mr. Kavi Kumar Khedo, University of Mauritius, Mauritius
Mr. Ravi Chandiran, Zagro Singapore Pte Ltd. Singapore
Mr. Milindkumar V. Sarode, Jawaharlal Darda Institute of Engineering and Technology, India
Dr. Shamimul Qamar, KSJ Institute of Engineering & Technology, India
Dr. C. Arun, Anna University, India
Assist. Prof. M.N.Birje, Basaveshwar Engineering College, India
Prof. Hamid Reza Naji, Department of Computer Enigneering, Shahid Beheshti University, Tehran, Iran
Assist. Prof. Debasis Giri, Department of Computer Science and Engineering, Haldia Institute of Technology
Subhabrata Barman, Haldia Institute of Technology, West Bengal
Mr. M. I. Lali, COMSATS Institute of Information Technology, Islamabad, Pakistan
Dr. Feroz Khan, Central Institute of Medicinal and Aromatic Plants, Lucknow, India
Mr. R. Nagendran, Institute of Technology, Coimbatore, Tamilnadu, India
Mr. Amnach Khawne, King Mongkut’s Institute of Technology Ladkrabang, Ladkrabang, Bangkok, Thailand

Dr. P. Chakrabarti, Sir Padampat Singhania University, Udaipur, India
Mr. Nafiz Imtiaz Bin Hamid, Islamic University of Technology (IUT), Bangladesh.
Shahab-A. Shamshirband, Islamic Azad University, Chalous, Iran
Prof. B. Priestly Shan, Anna Univeristy, Tamilnadu, India
Venkatramreddy Velma, Dept. of Bioinformatics, University of Mississippi Medical Center, Jackson MS USA
Akshi Kumar, Dept. of Computer Engineering, Delhi Technological University, India
Dr. Umesh Kumar Singh, Vikram University, Ujjain, India
Mr. Serguei A. Mokhov, Concordia University, Canada
Mr. Lai Khin Wee, Universiti Teknologi Malaysia, Malaysia
Dr. Awadhesh Kumar Sharma, Madan Mohan Malviya Engineering College, India
Mr. Syed R. Rizvi, Analytical Services & Materials, Inc., USA
Dr. S. Karthik, SNS Collegeof Technology, India
Mr. Syed Qasim Bukhari, CIMET (Universidad de Granada), Spain
Mr. A.D.Potgantwar, Pune University, India
Dr. Himanshu Aggarwal, Punjabi University, India
Mr. Rajesh Ramachandran, Naipunya Institute of Management and Information Technology, India
Dr. K.L. Shunmuganathan, R.M.K Engg College , Kavaraipettai ,Chennai
Dr. Prasant Kumar Pattnaik, KIST, India.
Dr. Ch. Aswani Kumar, VIT University, India
Mr. Ijaz Ali Shoukat, King Saud University, Riyadh KSA
Mr. Arun Kumar, Sir Padam Pat Singhania University, Udaipur, Rajasthan
Mr. Muhammad Imran Khan, Universiti Teknologi PETRONAS, Malaysia
Dr. Natarajan Meghanathan, Jackson State University, Jackson, MS, USA
Mr. Mohd Zaki Bin Mas'ud, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia
Prof. Dr. R. Geetharamani, Dept. of Computer Science and Eng., Rajalakshmi Engineering College, India
Dr. Smita Rajpal, Institute of Technology and Management, Gurgaon, India
Dr. S. Abdul Khader Jilani, University of Tabuk, Tabuk, Saudi Arabia
Mr. Syed Jamal Haider Zaidi, Bahria University, Pakistan
Dr. N. Devarajan, Government College of Technology,Coimbatore, Tamilnadu, INDIA
Mr. R. Jagadeesh Kannan, RMK Engineering College, India
Mr. Deo Prakash, Shri Mata Vaishno Devi University, India
Mr. Mohammad Abu Naser, Dept. of EEE, IUT, Gazipur, Bangladesh
Assist. Prof. Prasun Ghosal, Bengal Engineering and Science University, India
Mr. Md. Golam Kaosar, School of Engineering and Science, Victoria University, Melbourne City, Australia
Mr. R. Mahammad Shafi, Madanapalle Institute of Technology & Science, India
Dr. F.Sagayaraj Francis, Pondicherry Engineering College,India
Dr. Ajay Goel, HIET , Kaithal, India
Mr. Nayak Sunil Kashibarao, Bahirji Smarak Mahavidyalaya, India
Mr. Suhas J Manangi, Microsoft India
Dr. Kalyankar N. V., Yeshwant Mahavidyalaya, Nanded , India
Dr. K.D. Verma, S.V. College of Post graduate studies & Research, India
Dr. Amjad Rehman, University Technology Malaysia, Malaysia

Mr. Rachit Garg, L K College, Jalandhar, Punjab
Mr. J. William, M.A.M college of Engineering, Trichy, Tamilnadu,India
Prof. Jue-Sam Chou, Nanhua University, College of Science and Technology, Taiwan
Dr. Thorat S.B., Institute of Technology and Management, India
Mr. Ajay Prasad, Sir Padampat Singhania University, Udaipur, India
Dr. Kamaljit I. Lakhtaria, Atmiya Institute of Technology & Science, India
Mr. Syed Rafiul Hussain, Ahsanullah University of Science and Technology, Bangladesh
Mrs Fazeela Tunnisa, Najran University, Kingdom of Saudi Arabia
Mrs Kavita Taneja, Maharishi Markandeshwar University, Haryana, India
Mr. Maniyar Shiraz Ahmed, Najran University, Najran, KSA
Mr. Anand Kumar, AMC Engineering College, Bangalore
Dr. Rakesh Chandra Gangwar, Beant College of Engg. & Tech., Gurdaspur (Punjab) India
Dr. V V Rama Prasad, Sree Vidyanikethan Engineering College, India
Assist. Prof. Neetesh Kumar Gupta, Technocrats Institute of Technology, Bhopal (M.P.), India
Mr. Ashish Seth, Uttar Pradesh Technical University, Lucknow ,UP India
Dr. V V S S S Balaram, Sreenidhi Institute of Science and Technology, India
Mr Rahul Bhatia, Lingaya's Institute of Management and Technology, India
Prof. Niranjan Reddy. P, KITS , Warangal, India
Prof. Rakesh. Lingappa, Vijetha Institute of Technology, Bangalore, India
Dr. Mohammed Ali Hussain, Nimra College of Engineering & Technology, Vijayawada, A.P., India
Dr. A.Srinivasan, MNM Jain Engineering College, Rajiv Gandhi Salai, Thorapakkam, Chennai
Mr. Rakesh Kumar, M.M. University, Mullana, Ambala, India
Dr. Lena Khaled, Zarqa Private University, Aman, Jordon
Ms. Supriya Kapoor, Patni/Lingaya's Institute of Management and Tech., India
Dr. Tossapon Boongoen , Aberystwyth University, UK
Dr . Bilal Alatas, Firat University, Turkey
Assist. Prof. Jyoti Praaksh Singh , Academy of Technology, India
Dr. Ritu Soni, GNG College, India
Dr . Mahendra Kumar , Sagar Institute of Research & Technology, Bhopal, India.
Dr. Binod Kumar, Lakshmi Narayan College of Tech.(LNCT)Bhopal India
Dr. Muzhir Shaban Al-Ani, Amman Arab University Amman – Jordan
Dr. T.C. Manjunath , ATRIA Institute of Tech, India
Mr. Muhammad Zakarya, COMSATS Institute of Information Technology (CIIT), Pakistan
Assist. Prof. Harmunish Taneja, M. M. University, India
Dr. Chitra Dhawale , SICSR, Model Colony, Pune, India
Mrs Sankari Muthukaruppan, Nehru Institute of Engineering and Technology, Anna University, India
Mr. Aaqif Afzaal Abbasi, National University Of Sciences And Technology, Islamabad
Prof. Ashutosh Kumar Dubey, Trinity Institute of Technology and Research Bhopal, India
Mr. G. Appasami, Dr. Pauls Engineering College, India
Mr. M Yasin, National University of Science and Tech, karachi (NUST), Pakistan
Mr. Yaser Miaji, University Utara Malaysia, Malaysia
Mr. Shah Ahsanul Haque, International Islamic University Chittagong (IIUC), Bangladesh

Prof. (Dr) Syed Abdul Sattar, Royal Institute of Technology & Science, India
Dr. S. Sasikumar, Roever Engineering College
Assist. Prof. Monit Kapoor, Maharishi Markandeshwar University, India
Mr. Nwaocha Vivian O, National Open University of Nigeria
Dr. M. S. Vijaya, GR Govindarajulu School of Applied Computer Technology, India
Assist. Prof. Chakresh Kumar, Manav Rachna International University, India
Mr. Kunal Chadha , R&D Software Engineer, Gemalto, Singapore
Mr. Mueen Uddin, Universiti Teknologi Malaysia, UTM , Malaysia
Dr. Dhuha Basheer abdullah, Mosul university, Iraq
Mr. S. Audithan, Annamalai University, India
Prof. Vijay K Chaudhari, Technocrats Institute of Technology , India
Associate Prof. Mohd Ilyas Khan, Technocrats Institute of Technology , India
Dr. Vu Thanh Nguyen, University of Information Technology, HoChiMinh City, VietNam
Assist. Prof. Anand Sharma, MITS, Lakshmangarh, Sikar, Rajasthan, India
Prof. T V Narayana Rao, HITAM Engineering college, Hyderabad
Mr. Deepak Gour, Sir Padampat Singhania University, India
Assist. Prof. Amutharaj Joyson, Kalasalingam University, India
Mr. Ali Balador, Islamic Azad University, Iran
Mr. Mohit Jain, Maharaja Surajmal Institute of Technology, India
Mr. Dilip Kumar Sharma, GLA Institute of Technology & Management, India
Dr. Debojyoti Mitra, Sir padampat Singhania University, India
Dr. Ali Dehghantanha, Asia-Pacific University College of Technology and Innovation, Malaysia
Mr. Zhao Zhang, City University of Hong Kong, China
Prof. S.P. Setty, A.U. College of Engineering, India
Prof. Patel Rakeshkumar Kantilal, Sankalchand Patel College of Engineering, India
Mr. Biswajit Bhowmik, Bengal College of Engineering & Technology, India
Mr. Manoj Gupta, Apex Institute of Engineering & Technology, India
Assist. Prof. Ajay Sharma, Raj Kumar Goel Institute Of Technology, India
Assist. Prof. Ramveer Singh, Raj Kumar Goel Institute of Technology, India
Dr. Hanan Elazhary, Electronics Research Institute, Egypt
Dr. Hosam I. Faiq, USM, Malaysia
Prof. Dipti D. Patil, MAEER's MIT College of Engg. & Tech, Pune, India
Assist. Prof. Devendra Chack, BCT Kumaon engineering College Dwarahat Almora, India
Prof. Manpreet Singh, M. M. Engg. College, M. M. University, India
Assist. Prof. M. Sadiq ali Khan, University of Karachi, Pakistan
Mr. Prasad S. Halgaonkar, MIT - College of Engineering, Pune, India
Dr. Imran Ghani, Universiti Teknologi Malaysia, Malaysia
Prof. Varun Kumar Kakar, Kumaon Engineering College, Dwarahat, India
Assist. Prof. Nisheeth Joshi, Apaji Institute, Banasthali University, Rajasthan, India
Associate Prof. Kunwar S. Vaisla, VCT Kumaon Engineering College, India
Prof Anupam Choudhary, Bhilai School Of Engg.,Bhilai (C.G.),India
Mr. Divya Prakash Shrivastava, Al Jabal Al garbi University, Zawya, Libya

Associate Prof. Dr. V. Radha, Avinashilingam Deemed university for women, Coimbatore.
Dr. Kasarapu Ramani, JNT University, Anantapur, India
Dr. Anuraag Awasthi, Jayoti Vidyapeeth Womens University, India
Dr. C G Ravichandran, R V S College of Engineering and Technology, India
Dr. Mohamed A. Deriche, King Fahd University of Petroleum and Minerals, Saudi Arabia
Mr. Abbas Karimi, Universiti Putra Malaysia, Malaysia
Mr. Amit Kumar, Jaypee University of Engg. and Tech., India
Dr. Nikolai Stoianov, Defense Institute, Bulgaria
Assist. Prof. S. Ranichandra, KSR College of Arts and Science, Tiruchencode
Mr. T.K.P. Rajagopal, Diamond Horse International Pvt Ltd, India
Dr. Md. Ekramul Hamid, Rajshahi University, Bangladesh
Mr. Hemanta Kumar Kalita , TATA Consultancy Services (TCS), India
Dr. Messaouda Azzouzi, Ziane Achour University of Djelfa, Algeria
Prof. (Dr.) Juan Jose Martinez Castillo, "Gran Mariscal de Ayacucho" University and Acantelys research Group, Venezuela
Dr. Jatinderkumar R. Saini, Narmada College of Computer Application, India
Dr. Babak Bashari Rad, University Technology of Malaysia, Malaysia
Dr. Nighat Mir, Effat University, Saudi Arabia
Prof. (Dr.) G.M.Nasira, Sasurie College of Engineering, India
Mr. Varun Mittal, Gemalto Pte Ltd, Singapore
Assist. Prof. Mrs P. Banumathi, Kathir College Of Engineering, Coimbatore
Assist. Prof. Quan Yuan, University of Wisconsin-Stevens Point, US
Dr. Pranam Paul, Narula Institute of Technology, Agarpara, West Bengal, India
Assist. Prof. J. Ramkumar, V.L.B Janakiammal college of Arts & Science, India
Mr. P. Sivakumar, Anna university, Chennai, India
Mr. Md. Humayun Kabir Biswas, King Khalid University, Kingdom of Saudi Arabia
Mr. Mayank Singh, J.P. Institute of Engg & Technology, Meerut, India
HJ. Kamaruzaman Jusoff, Universiti Putra Malaysia
Mr. Nikhil Patrick Lobo, CADES, India
Dr. Amit Wason, Rayat-Bahra Institute of Engineering & Boi-Technology, India
Dr. Rajesh Shrivastava, Govt. Benazir Science & Commerce College, Bhopal, India
Assist. Prof. Vishal Bharti, DCE, Gurgaon
Mrs. Sunita Bansal, Birla Institute of Technology & Science, India
Dr. R. Sudhakar, Dr.Mahalingam college of Engineering and Technology, India
Dr. Amit Kumar Garg, Shri Mata Vaishno Devi University, Katra(J&K), India
Assist. Prof. Raj Gaurang Tiwari, AZAD Institute of Engineering and Technology, India
Mr. Hamed Taherdoost, Tehran, Iran
Mr. Amin Daneshmand Malayeri, YRC, IAU, Malayer Branch, Iran
Mr. Shantanu Pal, University of Calcutta, India
Dr. Terry H. Walcott, E-Promag Consultancy Group, United Kingdom
Dr. Ezekiel U OKIKE, University of Ibadan, Nigeria
Mr. P. Mahalingam, Caledonian College of Engineering, Oman

Dr. Mahmoud M. A. Abd Ellatif, Mansoura University, Egypt
Prof. Kunwar S. Vaisla, BCT Kumaon Engineering College, India
Prof. Mahesh H. Panchal, Kalol Institute of Technology & Research Centre, India
Mr. Muhammad Asad, Technical University of Munich, Germany
Mr. AliReza Shams Shafigh, Azad Islamic university, Iran
Prof. S. V. Nagaraj, RMK Engineering College, India
Mr. Ashikali M Hasan, Senior Researcher, CelNet security, India
Dr. Adnan Shahid Khan, University Technology Malaysia, Malaysia
Mr. Prakash Gajanan Burade, Nagpur University/ITM college of engg, Nagpur, India
Dr. Jagdish B.Helonde, Nagpur University/ITM college of engg, Nagpur, India
Professor, Doctor BOUHORMA Mohammed, Univertsity Abdelmalek Essaadi, Morocco
Mr. K. Thirumalaivasan, Pondicherry Engg. College, India
Mr. Umbarkar Anantkumar Janardan, Walchand College of Engineering, India
Mr. Ashish Chaurasia, Gyan Ganga Institute of Technology & Sciences, India
Mr. Sunil Taneja, Kurukshetra University, India
Mr. Fauzi Adi Rafrastara, Dian Nuswantoro University, Indonesia
Dr. Yaduvir Singh, Thapar University, India
Dr. Ioannis V. Koskosas, University of Western Macedonia, Greece
Dr. Vasantha Kalyani David, Avinashilingam University for women, Coimbatore
Dr. Ahmed Mansour Manasrah, Universiti Sains Malaysia, Malaysia
Miss. Nazanin Sadat Kazazi, University Technology Malaysia, Malaysia
Mr. Saeed Rasouli Heikalabad, Islamic Azad University - Tabriz Branch, Iran
Assoc. Prof. Dhirendra Mishra, SVKM's NMIMS University, India
Prof. Shapoor Zarei, UAE Inventors Association, UAE
Prof. B.Raja Sarath Kumar, Lenora College of Engineering, India
Dr. Bashir Alam, Jamia millia Islamia, Delhi, India
Prof. Anant J Umbarkar, Walchand College of Engg., India
Assist. Prof. B. Bharathi, Sathyabama University, India
Dr. Fokrul Alom Mazarbhuiya, King Khalid University, Saudi Arabia
Prof. T.S.Jeyali Laseeth, Anna University of Technology, Tirunelveli, India
Dr. M. Balraju, Jawahar Lal Nehru Technological University Hyderabad, India
Dr. Vijayalakshmi M. N., R.V.College of Engineering, Bangalore
Prof. Walid Moudani, Lebanese University, Lebanon
Dr. Saurabh Pal, VBS Purvanchal University, Jaunpur, India
Associate Prof. Suneet Chaudhary, Dehradun Institute of Technology, India
Associate Prof. Dr. Manuj Darbari, BBD University, India
Ms. Prema Selvaraj, K.S.R College of Arts and Science, India
Assist. Prof. Ms.S.Sasikala, KSR College of Arts & Science, India
Mr. Sukhvinder Singh Deora, NC Institute of Computer Sciences, India
Dr. Abhay Bansal, Amity School of Engineering & Technology, India
Ms. Sumita Mishra, Amity School of Engineering and Technology, India
Professor S. Viswanadha Raju, JNT University Hyderabad, India

Mr. Asghar Shahrzad Khashandarag, Islamic Azad University Tabriz Branch, India
Mr. Manoj Sharma, Panipat Institute of Engg. & Technology, India
Mr. Shakeel Ahmed, King Faisal University, Saudi Arabia
Dr. Mohamed Ali Mahjoub, Institute of Engineer of Monastir, Tunisia
Mr. Adri Jovin J.J., SriGuru Institute of Technology, India
Dr. Sukumar Senthilkumar, Universiti Sains Malaysia, Malaysia
Mr. Rakesh Bharati, Dehradun Institute of Technology Dehradun, India
Mr. Shervan Fekri Ershad, Shiraz International University, Iran
Mr. Md. Safiqul Islam, Daffodil International University, Bangladesh
Mr. Mahmudul Hasan, Daffodil International University, Bangladesh
Prof. Mandakini Tayade, UIT, RGTU, Bhopal, India
Ms. Sarla More, UIT, RGTU, Bhopal, India
Mr. Tushar Hrishikesh Jaware, R.C. Patel Institute of Technology, Shirpur, India
Ms. C. Divya, Dr G R Damodaran College of Science, Coimbatore, India
Mr. Fahimuddin Shaik, Annamacharya Institute of Technology & Sciences, India
Dr. M. N. Giri Prasad, JNTUCE,Pulivendula, A.P., India
Assist. Prof. Chintan M Bhatt, Charotar University of Science And Technology, India
Prof. Sahista Machchhar, Marwadi Education Foundation's Group of institutions, India
Assist. Prof. Navnish Goel, S. D. College Of Enginnering & Technology, India
Mr. Khaja Kamaluddin, Sirt University, Sirt, Libya
Mr. Mohammad Zaidul Karim, Daffodil International, Bangladesh
Mr. M. Vijayakumar, KSR College of Engineering, Tiruchengode, India
Mr. S. A. Ahsan Rajon, Khulna University, Bangladesh
Dr. Muhammad Mohsin Nazir, LCW University Lahore, Pakistan
Mr. Mohammad Asadul Hoque, University of Alabama, USA
Mr. P.V.Sarathchand, Indur Institute of Engineering and Technology, India
Mr. Durgesh Samadhiya, Chung Hua University, Taiwan
Dr Venu Kuthadi, University of Johannesburg, Johannesburg, RSA
Dr. (Er) Jasvir Singh, Guru Nanak Dev University, Amritsar, Punjab, India
Mr. Jasmin Cosic, Min. of the Interior of Una-sana canton, B&H, Bosnia and Herzegovina
Dr S. Rajalakshmi, Botho College, South Africa
Dr. Mohamed Sarrab, De Montfort University, UK
Mr. Basappa B. Kodada, Canara Engineering College, India
Assist. Prof. K. Ramana, Annamacharya Institute of Technology and Sciences, India
Dr. Ashu Gupta, Apeejay Institute of Management, Jalandhar, India
Assist. Prof. Shaik Rasool, Shadan College of Engineering & Technology, India
Assist. Prof. K. Suresh, Annamacharya Institute of Tech & Sci. Rajampet, AP, India
Dr . G. Singaravel, K.S.R. College of Engineering, India
Dr B. G. Geetha, K.S.R. College of Engineering, India
Assist. Prof. Kavita Choudhary, ITM University, Gurgaon
Dr. Mehrdad Jalali, Azad University, Mashhad, Iran
Megha Goel, Shamli Institute of Engineering and Technology, Shamli, India

Mr. Chi-Hua Chen, Institute of Information Management, National Chiao-Tung University, Taiwan (R.O.C.)
Assoc. Prof. A. Rajendran, RVS College of Engineering and Technology, India
Assist. Prof. S. Jaganathan, RVS College of Engineering and Technology, India
Assoc. Prof. A S N Chakravarthy, Sri Aditya Engineering College, India
Assist. Prof. Deepshikha Patel, Technocrat Institute of Technology, India
Assist. Prof. Maram Balajee, GMRIT, India
Assist. Prof. Monika Bhatnagar, TIT, India
Prof. Gaurang Panchal, Charotar University of Science & Technology, India
Prof. Anand K. Tripathi, Computer Society of India
Prof. Jyoti Chaudhary, High Performance Computing Research Lab, India
Assist. Prof. Supriya Raheja, ITM University, India
Dr. Pankaj Gupta, Microsoft Corporation, U.S.A.
Assist. Prof. Panchamukesh Chandaka, Hyderabad Institute of Tech. & Management, India
Prof. Mohan H.S, SJB Institute Of Technology, India
Mr. Hossein Malekinezhad, Islamic Azad University, Iran
Mr. Zatin Gupta, Universti Malaysia, Malaysia
Assist. Prof. Amit Chauhan, Phonics Group of Institutions, India
Assist. Prof. Ajal A. J., METS School Of Engineering, India
Mrs. Omowunmi Omobola Adeyemo, University of Ibadan, Nigeria
Dr. Bharat Bhushan Agarwal, I.F.T.M. University, India
Md. Nazrul Islam, University of Western Ontario, Canada
Tushar Kanti, L.N.C.T, Bhopal, India
Er. Aumreesh Kumar Saxena, SIRTs College Bhopal, India
Mr. Mohammad Monirul Islam, Daffodil International University, Bangladesh
Dr. Kashif Nisar, University Utara Malaysia, Malaysia
Dr. Wei Zheng, Rutgers Univ/ A10 Networks, USA
Associate Prof. Rituraj Jain, Vyas Institute of Engg & Tech, Jodhpur – Rajasthan
Assist. Prof. Apoorvi Sood, I.T.M. University, India
Dr. Kayhan Zrar Ghafoor, University Technology Malaysia, Malaysia
Mr. Swapnil Soner, Truba Institute College of Engineering & Technology, Indore, India
Ms. Yogita Gigras, I.T.M. University, India
Associate Prof. Neelima Sadineni, Pydha Engineering College, India Pydha Engineering College
Assist. Prof. K. Deepika Rani, HITAM, Hyderabad
Ms. Shikha Maheshwari, Jaipur Engineering College & Research Centre, India
Prof. Dr V S Giridhar Akula, Avanthi's Scientific Tech. & Research Academy, Hyderabad
Prof. Dr.S.Saravanan, Muthayammal Engineering College, India
Mr. Mehdi Golsorkhatabar Amiri, Islamic Azad University, Iran
Prof. Amit Sadanand Savyanavar, MITCOE, Pune, India
Assist. Prof. P.Oliver Jayaprakash, Anna University,Chennai
Assist. Prof. Ms. Sujata, ITM University, Gurgaon, India
Dr. Asoke Nath, St. Xavier's College, India
Mr. Masoud Rafighi, Islamic Azad University, Iran

Assist. Prof. RamBabu Pemula, NIMRA College of Engineering & Technology, India
Assist. Prof. Ms Rita Chhikara, ITM University, Gurgaon, India
Mr. Sandeep Maan, Government Post Graduate College, India
Prof. Dr. S. Muralidharan, Mepco Schlenk Engineering College, India
Associate Prof. T.V.Sai Krishna, QIS College of Engineering and Technology, India
Mr. R. Balu, Bharathiar University, Coimbatore, India
Assist. Prof. Shekhar. R, Dr.SM College of Engineering, India
Prof. P. Senthilkumar, Vivekanandha Institue of Engineering And Techology For Woman, India
Mr. M. Kamarajan, PSNA College of Engineering & Technology, India
Dr. Angajala Srinivasa Rao, Jawaharlal Nehru Technical University, India
Assist. Prof. C. Venkatesh, A.I.T.S, Rajampet, India
Mr. Afshin Rezakhani Roozbahani, Ayatollah Boroujerdi University, Iran
Mr. Laxmi chand, SCTL, Noida, India
Dr. Dr. Abdul Hannan, Vivekanand College, Aurangabad
Prof. Mahesh Panchal, KITRC, Gujarat
Dr. A. Subramani, K.S.R. College of Engineering, Tiruchengode
Assist. Prof. Prakash M, Rajalakshmi Engineering College, Chennai, India
Assist. Prof. Akhilesh K Sharma, Sir Padampat Singhania University, India
Ms. Varsha Sahni, Guru Nanak Dev Engineering College, Ludhiana, India
Associate Prof. Trilochan Rout, NM Institute Of Engineering And Technlogy, India
Mr. Srikanta Kumar Mohapatra, NMIET, Orissa, India
Mr. Waqas Haider Bangyal, Iqra University Islamabad, Pakistan
Dr. S. Vijayaragavan, Christ College of Engineering and Technology, Pondicherry, India
Prof. Elboukhari Mohamed, University Mohammed First, Oujda, Morocco
Dr. Muhammad Asif Khan, King Faisal University, Saudi Arabia
Dr. Nagy Ramadan Darwish Omran, Cairo University, Egypt.
Assistant Prof. Anand Nayyar, KCL Institute of Management and Technology, India
Mr. G. Premsankar, Ericcson, India
Assist. Prof. T. Hemalatha, VELS University, India
Prof. Tejaswini Apte, University of Pune, India
Dr. Edmund Ng Giap Weng, Universiti Malaysia Sarawak, Malaysia
Mr. Mahdi Nouri, Iran University of Science and Technology, Iran
Associate Prof. S. Asif Hussain, Annamacharya Institute of technology & Sciences, India
Mrs. Kavita Pabreja, Maharaja Surajmal Institute (an affiliate of GGSIP University), India
Mr. Vorugunti Chandra Sekhar, DA-IICT, India
Mr. Muhammad Najmi Ahmad Zabidi, Universiti Teknologi Malaysia, Malaysia
Dr. Aderemi A. Atayero, Covenant University, Nigeria
Assist. Prof. Osama Sohaib, Balochistan University of Information Technology, Pakistan
Assist. Prof. K. Suresh, Annamacharya Institute of Technology and Sciences, India
Mr. Hassen Mohammed Abduallah Alsafi, International Islamic University Malaysia (IIUM) Malaysia
Mr. Robail Yasrab, Virtual University of Pakistan, Pakistan
Mr. R. Balu, Bharathiar University, Coimbatore, India

Prof. Anand Nayyar, KCL Institute of Management and Technology, Jalandhar
Assoc. Prof. Vivek S Deshpande, MIT College of Engineering, India
Prof. K. Saravanan, Anna university Coimbatore, India
Dr. Ravendra Singh, MJP Rohilkhand University, Bareilly, India
Mr. V. Mathivanan, IBRA College of Technology, Sultanate of OMAN
Assoc. Prof. S. Asif Hussain, AITS, India
Assist. Prof. C. Venkatesh, AITS, India
Mr. Sami Ulhaq, SZABIST Islamabad, Pakistan
Dr. B. Justus Rabi, Institute of Science & Technology, India
Mr. Anuj Kumar Yadav, Dehradun Institute of technology, India
Mr. Alejandro Mosquera, University of Alicante, Spain
Assist. Prof. Arjun Singh, Sir Padampat Singhania University (SPSU), Udaipur, India
Dr. Smriti Agrawal, JB Institute of Engineering and Technology, Hyderabad
Assist. Prof. Swathi Sambangi, Visakha Institute of Engineering and Technology, India
Ms. Prabhjot Kaur, Guru Gobind Singh Indraprastha University, India
Mrs. Samaher AL-Hothali, Yanbu University College, Saudi Arabia
Prof. Rajneeshkaur Bedi, MIT College of Engineering, Pune, India
Mr. Hassen Mohammed Abduallah Alsafi, International Islamic University Malaysia (IIUM)
Dr. Wei Zhang, Amazon.com, Seattle, WA, USA
Mr. B. Santhosh Kumar, C S I College of Engineering, Tamil Nadu
Dr. K. Reji Kumar, , N S S College, Pandalam, India
Assoc. Prof. K. Seshadri Sastry, EIILM University, India
Mr. Kai Pan, UNC Charlotte, USA
Mr. Ruikar Sachin, SGGSIET, India
Prof. (Dr.) Vinodani Katiyar, Sri Ramswaroop Memorial University, India
Assoc. Prof., M. Giri, Sreenivasa Institute of Technology and Management Studies, India
Assoc. Prof. Labib Francis Gergis, Misr Academy for Engineering and Technology (MET), Egypt
Assist. Prof. Amanpreet Kaur, ITM University, India
Assist. Prof. Anand Singh Rajawat, Shri Vaishnav Institute of Technology & Science, Indore
Mrs. Hadeel Saleh Haj Aliwi, Universiti Sains Malaysia (USM), Malaysia
Dr. Abhay Bansal, Amity University, India
Dr. Mohammad A. Mezher, Fahad Bin Sultan University, KSA
Assist. Prof. Nidhi Arora, M.C.A. Institute, India
Prof. Dr. P. Suresh, Karpagam College of Engineering, Coimbatore, India
Dr. Kannan Balasubramanian, Mepco Schlenk Engineering College, India
Dr. S. Sankara Gomathi, Panimalar Engineering college, India
Prof. Anil kumar Suthar, Gujarat Technological University, L.C. Institute of Technology, India
Assist. Prof. R. Hubert Rajan, NOORUL ISLAM UNIVERSITY, India
Assist. Prof. Dr. Jyoti Mahajan, College of Engineering & Technology
Assist. Prof. Homam Reda El-Taj, College of Network Engineering, Saudi Arabia & Malaysia
Mr. Bijan Paul, Shahjalal University of Science & Technology, Bangladesh
Assoc. Prof. Dr. Ch V Phani Krishna, KL University, India

Dr. Vishal Bhatnagar, Ambedkar Institute of Advanced Communication Technologies & Research, India
Dr. Lamri LAOUAMER, Al Qassim University, Dept. Info. Systems & European University of Brittany, Dept. Computer Science, UBO, Brest, France
Prof. Ashish Babanrao Sasankar, G.H.Raisoni Institute Of Information Technology, India
Prof. Pawan Kumar Goel, Shamli Institute of Engineering and Technology, India
Mr. Ram Kumar Singh, S.V Subharti University, India
Assistant Prof. Sunish Kumar O S, Amaljyothi College of Engineering, India
Dr Sanjay Bhargava, Banasthali University, India

CALL FOR PAPERS
International Journal of Computer Science and Information Security
January - December
IJCSIS 2012
ISSN: 1947-5500
http://sites.google.com/site/ijcsis/

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2011 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

Track A: Security

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity
Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security ,Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc,), Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on
its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, **Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

Track B: Computer Science

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, Embeded Computer System, Advanced Control Systems, and Intelligent Control : Advanced control and measurement, computer and microprocessor-based control, signal processing, estimation and identification techniques, application specific IC's, nonlinear and adaptive control, optimal and robot control, intelligent control, evolutionary computing, and intelligent systems, instrumentation subject to critical conditions, automotive, marine and aero-space control and all other control applications, Intelligent Control System, Wiring/Wireless Sensor, Signal Control System. Sensors, Actuators and Systems Integration : Intelligent sensors and actuators, multisensor fusion, sensor array and multi-channel processing, micro/nano technology, microsensors and microactuators, instrumentation electronics, MEMS and system integration, wireless sensor, Network Sensor, Hybrid

Sensor, Distributed Sensor Networks. Signal and Image Processing : Digital signal processing theory, methods, DSP implementation, speech processing, image and multidimensional signal processing, Image analysis and processing, Image and Multimedia applications, Real-time multimedia signal processing, Computer vision, Emerging signal processing areas, Remote Sensing, Signal processing in education. Industrial Informatics: Industrial applications of neural networks, fuzzy algorithms, Neuro-Fuzzy application, bioInformatics, real-time computer control, real-time information systems, human-machine interfaces, CAD/CAM/CAT/CIM, virtual reality, industrial communications, flexible manufacturing systems, industrial automated process, Data Storage Management, Harddisk control, Supply Chain Management, Logistics applications, Power plant automation, Drives automation. Information Technology, Management of Information System : Management information systems, Information Management, Nursing information management, Information System, Information Technology and their application, Data retrieval, Data Base Management, Decision analysis methods, Information processing, Operations research, E-Business, E-Commerce, E-Government, Computer Business, Security and risk management, Medical imaging, Biotechnology, Bio-Medicine, Computer-based information systems in health care, Changing Access to Patient Information, Healthcare Management Information Technology. Communication/Computer Network, Transportation Application : On-board diagnostics, Active safety systems, Communication systems, Wireless technology, Communication application, Navigation and Guidance, Vision-based applications, Speech interface, Sensor fusion, Networking theory and technologies, Transportation information, Autonomous vehicle, Vehicle application of affective computing, Advance Computing technology and their application : Broadband and intelligent networks, Data Mining, Data fusion, Computational intelligence, Information and data security, Information indexing and retrieval, Information processing, Information systems and applications, Internet applications and performances, Knowledge based systems, Knowledge management, Software Engineering, Decision making, Mobile networks and services, Network management and services, Neural Network, Fuzzy logics, Neuro-Fuzzy, Expert approaches, Innovation Technology and Management : Innovation and product development, Emerging advances in business and its applications, Creativity in Internet management and retailing, B2B and B2C management, Electronic transceiver device for Retail Marketing Industries, Facilities planning and management, Innovative pervasive computing applications, Programming paradigms for pervasive systems, Software evolution and maintenance in pervasive systems, Middleware services and agent technologies, Adaptive, autonomic and context-aware computing, Mobile/Wireless computing systems and services in pervasive computing, Energy-efficient and green pervasive computing, Communication architectures for pervasive computing, Ad hoc networks for pervasive communications, Pervasive opportunistic communications and applications, Enabling technologies for pervasive systems (e.g., wireless BAN, PAN), Positioning and tracking technologies, Sensors and RFID in pervasive systems, Multimodal sensing and context for pervasive applications, Pervasive sensing, perception and semantic interpretation, Smart devices and intelligent environments, Trust, security and privacy issues in pervasive systems, User interfaces and interaction models, Virtual immersive communications, Wearable computers, Standards and interfaces for pervasive computing environments, Social and economic models for pervasive systems, Active and Programmable Networks, Ad Hoc & Sensor Network, Congestion and/or Flow Control, Content Distribution, Grid Networking, High-speed Network Architectures, Internet Services and Applications, Optical Networks, Mobile and Wireless Networks, Network Modeling and Simulation, Multicast, Multimedia Communications, Network Control and Management, Network Protocols, Network Performance, Network Measurement, Peer to Peer and Overlay Networks, Quality of Service and Quality of Experience, Ubiquitous Networks, Crosscutting Themes – Internet Technologies, Infrastructure, Services and Applications; Open Source Tools, Open Models and Architectures; Security, Privacy and Trust; Navigation Systems, Location Based Services; Social Networks and Online Communities; ICT Convergence, Digital Economy and Digital Divide, Neural Networks, Pattern Recognition, Computer Vision, Advanced Computing Architectures and New Programming Models, Visualization and Virtual Reality as Applied to Computational Science, Computer Architecture and Embedded Systems, Technology in Education, Theoretical Computer Science, Computing Ethics, Computing Practices & Applications

Authors are invited to submit papers through e-mail ijcsiseditor@gmail.com. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCSIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://sites.google.com/site/ijcsis/authors-notes .

© IJCSIS PUBLICATION 2012
ISSN 1947 5500
http://sites.google.com/site/ijcsis/